Check Point Safe@Office

Internet Security Appliance

User Guide

Version 8.2

Part No: 700797, November 2010

COPYRIGHT & TRADEMARKS

Copyright © 2010 SofaWare, All Rights Reserved. No part of this document may be reproduced in any form or by any means without written permission from SofaWare.

Information in this document is subject to change without notice and does not represent a commitment on part of SofaWare Technologies Ltd.

SofaWare, Safe@Home and Safe@Office are trademarks, service marks, or registered trademarks of SofaWare Technologies Ltd.

Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, Check Point Pointsec Protector, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Policy Lifecycle Management, Provider-1, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications. Any reproduction of this alert other than as an unmodified copy of this file requires authorization from Check Point. Permission to electronically redistribute this alert in its unmodified form is granted. All other rights, including the use of other media, are reserved by Check Point Software Technologies Inc.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with

modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

To receive the SofaWare GPL licensed code, contact info@sofaware.com.

SAFETY PRECAUTIONS

Carefully read the Safety Instructions the Installation and Operating Procedures provided in this User's Guide before attempting to install or operate the appliance. Failure to follow these instructions may result in damage to equipment and/or personal injuries.

- Before cleaning the appliance, unplug the power cord. Use only a soft cloth dampened with water for cleaning.
- When installing the appliance, ensure that the vents are not blocked.
- Do not place this product on an unstable surface or support. The product may fall, causing serious injury to a child or adult, as well as serious damage to the product.
- Do not use the appliance outdoors.
- Do not expose the appliance to liquid or moisture.

- Do not expose the appliance to extreme high or low temperatures.
- Do not disassemble or open the appliance. Failure to comply will void the warranty.
- Do not use any accessories other than those approved by Check Point. Failure to do so may result in loss of performance, damage to the product, fire, electric shock or injury, and will void the warranty.
- Route power adapter cords where they are not likely to be walked on or pinched by items placed on or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit the unit.
- Do not connect or disconnect power adapter cables and data transmission lines during thunderstorms.
- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard. Periodically examine the cord, and if its appearance indicates damage or deteriorated insulation, have it replaced by your service technician.
- If the unit or any part of it is damaged, disconnect the power plug and inform the responsible service personnel. Non-observance may result in damage to the router.

POWER ADAPTER

- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Use only the power adapter provided with your product. Check whether the device's set supply voltage is the same as the local supply voltage.
- To reduce risk of damage to the unit, remove it from the outlet by holding the power adapter rather than the cord.

SECURITY DISCLAIMER

The appliance provides your network with the highest level of security. However, no single security product can provide you with absolute protection. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

About This Guide ..... **ix**

Introduction **1**

About Your Check Point Safe@Office Appliance 1

Safe@Office Product Family 2

Safe@Office 1000N and 1000N ADSL Product Features 3

Safe@Office 1000NW and 1000NW ADSL Product Features 8

Safe@Office 500 and 500 ADSL Product Features 14

Safe@Office 500W and 500W ADSL Product Features 19

Wireless Features 25

Optional Security Services 26

Software Requirements 26

Getting to Know Your Safe@Office 1000N Appliance 27

Getting to Know Your Safe@Office 1000N ADSL Appliance 32

Getting to Know Your Safe@Office 1000NW Appliance 38

Getting to Know Your Safe@Office 1000NW ADSL Appliance 44

Getting to Know Your Safe@Office 500 Appliance 51

Getting to Know Your Safe@Office 500 ADSL Appliance 55

Getting to Know Your Safe@Office 500W Appliance 60

Getting to Know Your Safe@Office 500W ADSL Appliance 65

Contacting Technical Support 70

Safe@Office Security **71**

Introduction to Information Security 71

The Safe@Office Firewall 76

Installing and Setting Up Safe@Office **85**

Before You Install the Safe@Office Appliance 85

Appliance Installation 99

Wall Mounting the Safe@Office Appliance 103
Securing the Safe@Office Appliance against Theft 105
Setting Up the Safe@Office Appliance 107
Getting Started 111
Initial Login to the Safe@Office Portal 111
Logging in to the Safe@Office Portal 114
Accessing the Safe@Office Portal Remotely Using HTTPS 116
Using the Safe@Office Portal 118
Logging Out 123
Configuring the Internet Connection 125
Overview 125
Using the Internet Wizard 126
Using Internet Setup 141
Setting Up Modems 176
Viewing Internet Connection Information 188
Enabling/Disabling the Internet Connection 190
Using Quick Internet Connection/Disconnection 190
Configuring a Backup Internet Connection 191
Configuring WAN Load Balancing 192
Managing Your Network 195
Configuring Network Settings 195
Using the Internal DNS Server 224
Using Network Objects 227
Configuring Network Service Objects 237
Using Static Routes 241
Managing Ports 246

Using Bridges **259**
Overview 259
Workflow 265
Adding and Editing Bridges 266
Adding Internal Networks to Bridges 270
Adding Internet Connections to Bridges 274
Deleting Bridges 278
Configuring High Availability **281**
Overview 281
Configuring High Availability on a Gateway 284
Sample Implementation on Two Gateways 289
Using Traffic Shaper **293**
Overview 293
Setting Up Traffic Shaper 295
Predefined QoS Classes 296
Adding and Editing Classes 298
Viewing and Deleting Classes 302
Restoring Traffic Shaper Defaults 303
Working with Wireless Networks **305**
Overview 305
Configuring Wireless Networks 314
Troubleshooting Wireless Connectivity 342
Viewing Reports **345**
Viewing the Safe@Office Appliance Status 345
Using the Traffic Monitor 352
Viewing Computers 357
Viewing Connections 359

Viewing Network Statistics....362
Viewing the Routing Table....374
Viewing Wireless Station Statistics....376
Viewing Logs....379
Viewing the Event Log....379
Viewing the Security Log....383
Setting Your Security Policy....391
The Safe@Office Firewall Security Policy....391
Default Security Policy....393
Setting the Firewall Security Level....394
Configuring Servers....397
Using Rules....400
Using Port-Based Security....413
Using Secure HotSpot....419
Using NAT Rules....425
Using the EAP Authenticator....433
Using SmartDefense....449
Overview....449
Configuring SmartDefense....450
SmartDefense Categories....458
Resetting SmartDefense to its Defaults....503
Using Antivirus and Antispam Filtering....505
Overview....505
Using VStream Antivirus....507
Using VStream Antispam....525
Using Centralized Email Filtering....558

Using Web Content Filtering 565
Overview 565
Using Web Rules 567
Using Web Filtering 575
Customizing the Access Denied Page 582
Updating the Firmware 585
Overview 585
Using Software Updates 586
Updating the Firmware Manually 588
Using Subscription Services 591
Connecting to a Service Center 591
Viewing Services Information 597
Refreshing Your Service Center Connection 598
Configuring Your Account 599
Disconnecting from Your Service Center 599
Working With VPNs 601
Overview 601
Setting Up Your Safe@Office Appliance as a VPN Server 607
Adding and Editing VPN Sites 621
Viewing and Deleting VPN Sites 654
Enabling/Disabling a VPN Site 654
Logging in to a Remote Access VPN Site 655
Logging Out of a Remote Access VPN Site 658
Using Certificates 658
Viewing VPN Tunnels 670
Viewing IKE Traces for VPN Connections 673
Viewing VPN Topology 674

Managing Users **677**
Changing Your Login Credentials 677
Adding and Editing Users 680
Adding Quick Guest HotSpot Users 685
Viewing and Deleting Users 686
Setting Up Remote VPN Access for Users 687
Using RADIUS Authentication 688
Configuring RADIUS Attributes 694
Using Remote Desktop **699**
Overview 699
Workflow 700
Configuring Remote Desktop 701
Configuring the Host Computer 704
Accessing a Remote Computer's Desktop 707
Controlling the Appliance via the Command Line **711**
Overview 711
Using the Safe@Office Portal 712
Using the Serial Console 714
Configuring SSH 717
Maintenance **720**
Viewing Firmware Status 720
Upgrading Your Software Product 722
Configuring a Gateway Hostname 724
Configuring Syslog Logging 726
Configuring HTTPS 728
Configuring SNMP 730
Setting the Time on the Appliance 735

Using Diagnostic Tools 738
Backing Up and Restoring the Safe@Office Appliance Configuration 752
Using Rapid Deployment 759
Resetting the Safe@Office Appliance to Defaults 762
Running Diagnostics 765
Rebooting the Safe@Office Appliance 766
Using Network Printers 767
Overview 767
Setting Up Network Printers 768
Configuring Computers to Use Network Printers 771
Viewing Network Printers 788
Changing Network Printer Ports 789
Resetting Network Printers 790
Troubleshooting 791
Connectivity 791
Service Center and Upgrades 795
Other Problems 796
Specifications 797
Technical Specifications 797
CE Declaration of Conformity 807
Glossary of Terms 819
Index 825

About This Guide

To make finding information in this guide easier, some types of information are marked with special symbols or formatting.

Boldface type is used for command and button names.

Note: Notes are denoted by indented text and preceded by the Note icon.

Warning: Warnings are denoted by indented text and preceded by the Warning icon.

Each task is marked with an icon indicating the Safe@Office product required to perform the task, as follows:

If this icon appears...	You can perform the task using these products...
500	Safe@Office 500 or Safe@Office 500W, with or without the Power Pack or ADSL
500W	Safe@Office 500W *only*, with or without the Power Pack or ADSL
1000N	Safe@Office 1000N or Safe@Office 1000NW, with or without the Power Pack or ADSL
1000NW	Safe@Office 1000NW *only*, with or without the Power Pack or ADSL
Power Pack	All products, with or without ADSL, *with the Power Pack only*
USB	All products *with USB ports*

	All products, with or without the Power Pack, *with ADSL only*
	All products, with or without the Power Pack, *without ADSL only*

Chapter 1

Introduction

This chapter introduces the Check Point Safe@Office appliance and this guide.

This chapter includes the following topics:

About Your Check Point Safe@Office Appliance 1
Safe@Office Product Family 2
Safe@Office 1000N and 1000N ADSL Product Features.....3
Safe@Office 1000NW and 1000NW ADSL Product Features 8
Safe@Office 500 and 500 ADSL Product Features 14
Safe@Office 500W and 500W ADSL Product Features.....19
Wireless Features.....25
Optional Security Services 26
Software Requirements 26
Getting to Know Your Safe@Office 1000N Appliance 27
Getting to Know Your Safe@Office 1000N ADSL Appliance.....32
Getting to Know Your Safe@Office 1000NW Appliance 38
Getting to Know Your Safe@Office 1000NW ADSL Appliance 44
Getting to Know Your Safe@Office 500 Appliance.....51
Getting to Know Your Safe@Office 500 ADSL Appliance.....55
Getting to Know Your Safe@Office 500W Appliance 60
Getting to Know Your Safe@Office 500W ADSL Appliance.....65
Contacting Technical Support 70

About Your Check Point Safe@Office Appliance

The Check Point Safe@Office appliance is a unified threat management (UTM) appliance that enables secure high-speed Internet access from the office. Developed and supported by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet, the Safe@Office product family includes both wired and wireless models, with and without an integrated ADSL modem. The Safe@Office firewall, based on the world-leading Check Point Embedded NGX Stateful Inspection technology, inspects and filters all incoming and outgoing traffic, blocking all unauthorized traffic.

The Safe@Office appliance also allows sharing your Internet connection among several PCs or other network devices, enabling advanced office networking and saving the cost of purchasing static IP addresses.

With the Safe@Office appliance, you can subscribe to additional security services available from select service providers, including firewall security and software updates, Antivirus, Antispam, Web Filtering, reporting, VPN management, and Dynamic DNS. By supporting integrated VPN capabilities, the Safe@Office appliance allows teleworkers and road warriors to securely connect to the office network, and enables secure interconnection of branch offices.

Safe@Office Product Family

The Safe@Office series includes the following hardware models:

- Safe@Office 1000N Internet Security Appliance
- Safe@Office 1000N ADSL Internet Security Appliance
- Safe@Office 1000NW Wireless Security Appliance
- Safe@Office 1000NW ADSL Wireless Security Appliance
- Safe@Office 500 Internet Security Appliance
- Safe@Office 500 ADSL Internet Security Appliance
- Safe@Office 500W Wireless Security Appliance
- Safe@Office 500W ADSL Wireless Internet Security Appliance

You can upgrade your Safe@Office appliance to include additional features without replacing the hardware by installing the Safe@Office Power Pack, and you can increase the number of licensed users by installing node upgrades. Contact your reseller for more details.

Safe@Office 1000N and 1000N ADSL Product Features

Table 1: Safe@Office 1000N and 1000N ADSL Features

Feature	Safe@Office 1000N	Safe@Office 1000N ADSL
SKU Prefix	CPSB-1000N-n	CPSB-1000N-n-ADSL
Concurrent Users	25/Unlimited	
Capacity		
Firewall Throughput	1 Gbps	
VPN Throughput	200 Mbps	
Concurrent Firewall Connections	60,000	
Hardware Features		
4-Port LAN Switch	Ethernet, 10/100/1000 Mbps	
WAN Port	Ethernet, 10/100/1000 Mbps	ADSL2+
ADSL Standards	—	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) Either: ANNEX A (ADSL over POTS) Or: ANNEX B (ADSL over ISDN)

DMZ/WAN2 Port	Ethernet / SFP, 10/100/1000 Mbps	
Dialup Backup	With external serial / USB modem	
Console Port (Serial)	✓	
ExpressCard Port	—	✓
Print Server	—	✓
USB 2.0 Ports	—	2
Firewall & Security Features		
Check Point Stateful Inspection Firewall	✓	
Application Intelligence	✓	
SmartDefense™ (IPS)	✓	
Network Address Translation (NAT)	✓	
Four Preset Security Policies	✓	
Anti-spoofing	✓	
Voice over IP Support	SIP, H.323	
Instant Messenger Blocking / Monitoring	✓	

P2P File Sharing Blocking / Monitoring	✓
Port-based and Tag-based VLAN	✓*
Port-based Security (802.1x)	✓*
EAP Authenticator	✓
Web Rules	✓
Secure HotSpot (Guest Access)	✓*
VPN	
VPN Tunnels	400
VPN Server with OfficeMode and RADIUS Support	Check Point VPN Clients, L2TP
Site-to-Site VPN Gateway	✓
Route-based VPN	✓
Backup VPN Gateways	✓
Remote Access VPN Client	SecuRemote / SecureClient / L2TP / Endpoint Connect

IPSEC Features	Hardware-accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSEC Compression, IPSEC NAT Traversal (NAT-T), IPSEC VPN Pass-through	
Networking		
Supported Internet Connection Methods	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, Dialup	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, EoA, PPPoA, IPoA, Dialup
Transparent Bridge Mode	✓	
Spanning Tree Protocol (STP)	✓	
Traffic Shaper (QoS)	Basic/Advanced*	
Traffic Monitoring	✓	
Dead Internet Connection Detection (DCD)	✓	
WAN Load Balancing	✓	
Backup Internet Connection	✓	
DHCP Server, Client, and Relay	✓	
DHCP Leases	1024	
DNS Server	✓	

MAC Cloning	✓
Network Address Translation (NAT) Rules	✓
Static Routes, Source Routes, and Service-Based Routes	✓
Ethernet Cable Type Recognition	✓
DiffServ Tagging	✓*
Automatic Gateway Failover (HA)	✓*
Multicast Routing	✓*
Dynamic Routing	✓*
Management	
Central Management	SMP
Local Management	HTTP / HTTPS / SSH / SNMP / Serial CLI
Remote Desktop	Integrated Microsoft Terminal Services Client
Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, Status Monitor, Traffic Monitor, My Computers Display, Connection Table Display, Network Interface Monitor, VPN Tunnel Monitor, Routing Table Display, Event Log, Security Log
NTP Automatic Time	✓

Setting	
Rapid Deployment	✓
Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop, Wall, or Rack Mounting**
Warranty	1 Year Hardware

* Requires Power Pack upgrade CPSB-1000-UPG-PPACK.

** Rack mounting requires the optional rack mounting kit (sold separately).

Safe@Office 1000NW and 1000NW ADSL Product Features

Table 2: Safe@Office 1000NW and 1000NW ADSL Features

Feature	Safe@Office 1000NW	Safe@Office 1000NW ADSL
SKU Prefix	CPSB-1000NW-n	CPSB-1000NW-n-ADSL
Concurrent Users	25/Unlimited	
Capacity		
Firewall Throughput	1 Gbps	
VPN Throughput	200 Mbps	
Concurrent Firewall Connections	60,000	

Hardware Features		
4-Port LAN Switch	Ethernet, 10/100/1000 Mbps	
WAN Port	Ethernet 10/100/1000 Mbps	ADSL2+
ADSL Standards	—	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) Either: ANNEX A (ADSL over POTS) Or: ANNEX B (ADSL over ISDN)
DMZ/WAN2 Port	Ethernet 10/100/1000 Mbps	
Dialup Backup	With external serial / USB modem	
Console Port (Serial)	✓	
ExpressCard Port	—	✓
Print Server	✓	
USB 2.0 Ports	2	1
Firewall & Security Features		
Check Point Stateful Inspection Firewall	✓	
Application	✓	

Intelligence	
SmartDefense™ (IPS)	✓
Network Address Translation (NAT)	✓
Four Preset Security Policies	✓
Anti-spoofing	✓
Voice over IP Support	SIP, H.323
Instant Messenger Blocking / Monitoring	✓
P2P File Sharing Blocking / Monitoring	✓
Port-based and Tag-based VLAN	✓*
Port-based Security (802.1x)	✓*
EAP Authenticator	✓
Web Rules	✓
Secure HotSpot (Guest Access)	✓*
VPN	
VPN Tunnels	400

VPN Server with OfficeMode and RADIUS Support	Check Point VPN Clients, L2TP	
Site-to-Site VPN Gateway	✓	
Route-based VPN	✓	
Backup VPN Gateways	✓	
Remote Access VPN Client	SecuRemote / SecureClient / L2TP / Endpoint Connect	
IPSEC Features	Hardware-accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSEC Compression, IPSEC NAT Traversal (NAT-T), IPSEC VPN Pass-through	
Networking		
Supported Internet Connection Methods	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, Dialup	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, EoA, PPPoA, IPoA, Dialup
Transparent Bridge Mode	✓	
Spanning Tree Protocol (STP)	✓	
Traffic Shaper (QoS)	Basic/Advanced*	
Traffic Monitoring	✓	

Dead Internet Connection Detection (DCD)	✓
WAN Load Balancing	✓
Backup Internet Connection	✓
DHCP Server, Client, and Relay	✓
DHCP Leases	1024
DNS Server	✓
MAC Cloning	✓
Network Address Translation (NAT) Rules	✓
Static Routes, Source Routes, and Service-Based Routes	✓
Ethernet Cable Type Recognition	✓
DiffServ Tagging	✓*
Automatic Gateway Failover (HA)	✓*
Multicast Routing	✓*

Dynamic Routing	✓*
Management	
Central Management	SMP
Local Management	HTTP / HTTPS / SSH / SNMP / Serial CLI
Remote Desktop	Integrated Microsoft Terminal Services Client
Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, Status Monitor, Traffic Monitor, My Computers Display, Connection Table Display, Network Interface Monitor, VPN Tunnel Monitor, Routing Table Display, Event Log, Security Log
NTP Automatic Time Setting	✓
Rapid Deployment	✓
Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop, Wall, or Rack Mounting**
Warranty	1 Year Hardware

* Requires Power Pack upgrade CPSB-1000-UPG-PPACK.

** Rack mounting requires the optional rack mounting kit (sold separately).

Safe@Office 500 and 500 ADSL Product Features

Table 3: Safe@Office 500 and 500 ADSL Features

Feature	Safe@Office 500	Safe@Office 500 ADSL
SKU Prefix	CPSB-500G-n	CPSB-500G-n-ADSL
Concurrent Users	5/25/U	
Capacity		
Firewall Throughput	190 Mbps	
VPN Throughput	35 Mbps	
Concurrent Firewall Connections	8,000	
Hardware Features		
4-Port LAN Switch	10/100 Mbps	
WAN Port	Ethernet, 10/100 Mbps	ADSL2+
ADSL Standards	—	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) Either: ANNEX A (ADSL over POTS) Or: ANNEX B (ADSL over ISDN)
DMZ/WAN2 Port	10/100 Mbps	

Dialup Backup	With external serial / USB modem	
Console Port (Serial)	✓	
Print Server	—	✓
USB 2.0 Ports	—	2
Firewall & Security Features		
Check Point Stateful Inspection Firewall	✓	
Application Intelligence	✓	
SmartDefense™ (IPS)	✓	
Network Address Translation (NAT)	✓	
Four Preset Security Policies	✓	
Anti-spoofing	✓	
Voice over IP Support	SIP, H.323	
Instant Messenger Blocking / Monitoring	✓	
P2P File Sharing Blocking / Monitoring	✓	

Port-based and Tag-based VLAN	✓*
Port-based Security (802.1x)	✓*
EAP Authenticator	✓
Web Rules	✓
Secure HotSpot (Guest Access)	✓*
VPN	
VPN Tunnels	100 (with Management)
VPN Server with OfficeMode and RADIUS Support	Check Point VPN Clients, L2TP
Site-to-Site VPN Gateway	✓
Route-based VPN	✓
Backup VPN Gateways	✓
Remote Access VPN Client	SecuRemote / SecureClient / L2TP / Endpoint Connect
IPSEC Features	Hardware-accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSEC Compression, IPSEC NAT Traversal (NAT-T), IPSEC VPN Pass-through

Networking		
Supported Internet Connection Methods	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, Dialup	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, EoA, PPPoA, IPoA, Dialup
Transparent Bridge Mode	✓	
Spanning Tree Protocol (STP)	✓	
Traffic Shaper (QoS)	Basic/Advanced*	
Traffic Monitoring	✓	
Dead Internet Connection Detection (DCD)	✓	
WAN Load Balancing	✓	
Backup Internet Connection	✓	
DHCP Server, Client, and Relay	✓	
DNS Server	✓	
MAC Cloning	✓	
Network Address Translation (NAT) Rules	✓	

Static Routes, Source Routes, and Service-Based Routes	✓
Ethernet Cable Type Recognition	✓
DiffServ Tagging	✓*
Automatic Gateway Failover (HA)	✓*
Multicast Routing	✓*
Dynamic Routing	✓*
Management	
Central Management	SMP
Local Management	HTTP / HTTPS / SSH / SNMP / Serial CLI
Remote Desktop	Integrated Microsoft Terminal Services Client
Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, Status Monitor, Traffic Monitor, My Computers Display, Connection Table Display, Network Interface Monitor, VPN Tunnel Monitor, Routing Table Display, Event Log, Security Log
NTP Automatic Time Setting	✓
Rapid Deployment	✓

Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop, Wall, or Rack Mounting**
Warranty	1 Year Hardware

* Requires Power Pack upgrade CPSB-500-UPG-PPACK.

** Rack mounting requires the optional rack mounting kit (sold separately).

Safe@Office 500W and 500W ADSL Product Features

Table 4: Safe@Office 500W and 500W ADSL Features

Feature	Safe@Office 500W	Safe@Office 500W ADSL
SKU Prefix	CPSB-500WG-n	CPSB-500WG-n-ADSL
Concurrent Users	5/25/U	
Capacity		
Firewall Throughput	190 Mbps	
VPN Throughput	35 Mbps	
Concurrent Firewall Connections	8,000	
Hardware Features		
4-Port LAN Switch	10/100 Mbps	

WAN Port	Ethernet, 10/100 Mbps	ADSL2+
ADSL Standards	—	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) Either: ANNEX A (ADSL over POTS) Or: ANNEX B (ADSL over ISDN)
DMZ/WAN2 Port	10/100 Mbps	
Dialup Backup	With external serial / USB modem	
Console Port (Serial)	✓	
Print Server	✓	
USB 2.0 Ports	2	
Firewall & Security Features		
Check Point Stateful Inspection Firewall	✓	
Application Intelligence	✓	
SmartDefense™ (IPS)	✓	
Network Address Translation (NAT)	✓	

Four Preset Security Policies	✓
Anti-spoofing	✓
Voice over IP Support	SIP, H.323
Instant Messenger Blocking / Monitoring	✓
P2P File Sharing Blocking / Monitoring	✓
Port-based and Tag-based VLAN	✓*
Port-based Security (802.1x)	✓*
EAP Authenticator	✓
Web Rules	✓
Secure HotSpot (Guest Access)	✓*
VPN	
VPN Tunnels	100 (with Management)
VPN Server with OfficeMode and RADIUS Support	Check Point VPN Clients, L2TP
Site-to-Site VPN Gateway	✓

Route-based VPN	✓	
Backup VPN Gateways	✓	
Remote Access VPN Client	SecuRemote / SecureClient / L2TP / Endpoint Connect	
IPSEC Features	Hardware-accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSEC Compression, IPSEC NAT Traversal (NAT-T), IPSEC VPN Pass-through	
Networking		
Supported Internet Connection Methods	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, Dialup	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, EoA, PPPoA, IPoA, Dialup
Transparent Bridge Mode	✓	
Spanning Tree Protocol (STP)	✓	
Traffic Shaper (QoS)	Basic/Advanced*	
Traffic Monitoring	✓	
Dead Internet Connection Detection (DCD)	✓	
WAN Load Balancing	✓	
Backup Internet	✓	

Connection	
DHCP Server, Client, and Relay	✓
DNS Server	✓
MAC Cloning	✓
Network Address Translation (NAT) Rules	✓
Static Routes, Source Routes, and Service-Based Routes	✓
Ethernet Cable Type Recognition	✓
DiffServ Tagging	✓*
Automatic Gateway Failover (HA)	✓*
Multicast Routing	✓*
Dynamic Routing	✓*
Management	
Central Management	SMP
Local Management	HTTP / HTTPS / SSH / SNMP / Serial CLI
Remote Desktop	Integrated Microsoft Terminal Services Client

Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, Status Monitor, Traffic Monitor, My Computers Display, Connection Table Display, Network Interface Monitor, VPN Tunnel Monitor, Routing Table Display, Event Log, Security Log
NTP Automatic Time Setting	✓
Rapid Deployment	✓
Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop, Wall, or Rack Mounting**
Warranty	1 Year Hardware

* Requires Power Pack upgrade CPSB-500-UPG-PPACK.

** Rack mounting requires the optional rack mounting kit (sold separately).

Wireless Features

Table 5: Safe@Office Wireless Features

Feature	Safe@Office 500W / Safe@Office 500W ADSL	Safe@Office 1000NW / Safe@Office 1000W ADSL
Wireless Protocols	802.11b (11 Mbps), 802.11g (54 Mbps), Super G (108 Mbps)**	802.11b (11 Mbps), 802.11g (54 Mbps), 802.11n (300 Mbps)
Wireless Security	VPN over Wireless, WEP, WPA2 (802.11i), WPA-Personal, WPA-Enterprise, 802.1x	
Wireless QoS (WMM)	✓	
Dual Diversity Antennas	✓	
Virtual Access Points (VAP)	✓*	
Wireless Distribution System (WDS) Links	✓*	
Wireless Range (Standard Mode)	Up to 100 m Indoors and 300 m Outdoors	
Wireless Range (XR Mode)**	Up to 300 m Indoors and 1 km Outdoors	

* Requires Power Pack upgrade CPSB-500-UPG-PPACK or CPSB-1000-UPG-PPACK, depending on series.

** Super G and XR mode are only available with select wireless network adapters. Actual ranges are subject to change in different environments.

Optional Security Services

The following subscription security services are available to Safe@Office owners by connecting to a Service Center:

- Firewall Security and Software Updates
- Web Filtering
- Email Antivirus and Antispam Protection
- VStream Embedded Antivirus Updates
- VStream Embedded Antispam Service
- Dynamic DNS Service
- VPN Management
- Security Reporting
- Vulnerability Scanning Service

These services require an additional purchase of subscription. For more information, contact your Check Point reseller.

Software Requirements

One of the following browsers:

- Microsoft Internet Explorer 6.0 or higher
- Netscape Navigator 6.0 and higher
- Mozilla Firefox

Note: For proper operation of the Safe@Office Portal, disable any pop-up blockers for http://my.firewall.

Getting to Know Your Safe@Office 1000N Appliance

1000N

Package Contents

The Safe@Office 1000N package includes the following:

- Safe@Office 1000N Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)

Network Requirements

- 10BaseT or 100BaseT or 1000BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

Figure 1: Safe@Office 1000N Appliance Rear Panel

The following table lists the Safe@Office 1000N appliance's rear panel elements.

Table 6: Safe@Office 1000N Appliance Rear Panel Elements

Label	Description
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the Internet
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.

Label	Description
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (10 seconds or until SYS LED begins to blink rapidly). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.

Front Panel

The Safe@Office 1000N appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 2: Safe@Office 1000N Appliance Front Panel

For an explanation of the Safe@Office 1000N appliance's status LEDs, see the table below.

Table 7: Safe@Office 1000N Appliance Status LEDs

LED	State	Explanation
Power	Off	Power off
	On (Green)	Normal operation
System	On (Red)	Boot failed or TFTP mode
	Flashing quickly (Red)	High temperature or system failure
	Flashing slowly (Orange)	Writing update to flash memory
	Flashing quickly (Green)	System boot in progress
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
Security	Off	Normal operation
	Flashing for 5 sec (Orange)	Virus blocked
	Flashing for 1 sec (Red)	Hacker attack blocked
GbE Status (WAN / DMZ / LAN 1-4)	1000Mbps Off, LINK/ACT Off	No Link
	1000Mbps Off, LINK/ACT On (Green)	10 Mbps link established for the corresponding port
	1000Mbps On (Orange), LINK/ACT On	100 Mbps link established for the corresponding port
	1000Mbps On (Green), LINK/ACT On	1000 Mbps link established for the corresponding port

	1000Mbps Off, LINK/ACT Flashing (Green)	10 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Orange), LINK/ACT Flashing (Green)	100 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Green), LINK/ACT Flashing (Green)	1000 Mbps link established for the corresponding port Data is being transmitted/received
VPN	Off	No VPN tunnel established
	On (Green)	VPN idle / No activity
	Flashing (Green)	VPN activity
RS232/Serial	Off	No data terminal connected
	On (Green)	Data terminal ready
	Flashing (Green)	Serial activity

Getting to Know Your Safe@Office 1000N ADSL Appliance

Package Contents

The Safe@Office 1000N ADSL package includes the following:

- Safe@Office 1000N ADSL Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT or 1000BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An ADSL line suitable for your appliance model:
  - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
  - For Annex B ADSL models, an ADSL over ISDN line (digital line)
- A splitter with a micro-filter, installed on all the jacks connected to the same phone line

- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

Figure 3: Safe@Office 1000N ADSL Appliance Rear Panel

The following table lists the Safe@Office 1000N ADSL appliance's rear panel elements.

Table 8: Safe@Office 1000N ADSL Appliance Rear Panel Elements

Label	Description
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
DMZ/ WAN2	DMZ/WAN2 switch: Two ports used for connecting a DMZ (Demilitarized Zone) computer or network: • An Ethernet port (RJ-45) on the left • An SFP (Small Form-factor Pluggable) port on the right Alternatively, can serve as a secondary WAN port or as a VLAN trunk. Only one of these ports can be used at a time.

Label	Description
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
USB	Two USB 2.0 ports used for connecting USB-based printers or modems
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (10 seconds or until the SYS LED begins to blink rapidly). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.

Side Panel

The side panel includes a slot for inserting an ExpressCard cellular modem.

Figure 4: Safe@Office 1000N ADSL Appliance Side Panel

Front Panel

The Safe@Office 1000N ADSL appliance includes several status LEDs that enable you to monitor the appliance's operation.

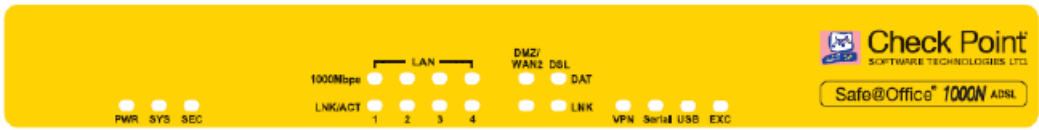


Figure 5: Safe@Office 1000N ADSL Appliance Front Panel

For an explanation of the Safe@Office 1000N ADSL appliance's status LEDs, see the table below.

Table 9: Safe@Office 1000N ADSL Appliance Status LEDs

LED	State	Explanation
Power	Off	Power off
	On (Green)	Normal operation
System	On (Red)	Boot failed or TFTP mode

	Flashing quickly (Red)	High temperature or system failure
	Flashing slowly (Orange)	Writing update to flash memory
	Flashing quickly (Green)	System boot in progress
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
Security	Off	Normal operation
	Flashing for 5 sec (Orange)	Virus blocked
	Flashing for 1 sec (Red)	Hacker attack blocked
GbE Status (LAN 1-4 / DMZ/WAN2)	1000Mbps Off, LINK/ACT Off	No Link
	1000Mbps Off, LINK/ACT On (Green)	10 Mbps link established for the corresponding port
	1000Mbps On (Orange), LINK/ACT On	100 Mbps link established for the corresponding port
	1000Mbps On (Green), LINK/ACT On	1000 Mbps link established for the corresponding port
	1000Mbps Off, LINK/ACT Flashing (Green)	10 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Orange), LINK/ACT Flashing (Green)	100 Mbps link established for the corresponding port Data is being transmitted/received

	1000Mbps On (Green), LINK/ACT Flashing (Green)	1000 Mbps link established for the corresponding port Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received
VPN	Off	No VPN tunnel established
	On (Green)	VPN idle / No activity
	Flashing (Green)	VPN activity
RS232/Serial	Off	No data terminal connected
	On (Green)	Data terminal ready
	Flashing (Green)	Serial activity
USB	Off	No USB device connected
	On (Green)	USB device connected
	Flashing (Green)	Activity on the USB device
EXC	Off	No ExpressCard connected
	On (Green)	ExpressCard connected
	Flashing (Green)	Activity on the ExpressCard

Getting to Know Your Safe@Office 1000NW Appliance

Package Contents

The Safe@Office 1000NW package includes the following:

- Safe@Office 1000NW Wireless Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- Two antennas
- USB extension cable

Network Requirements

- 10BaseT or 100BaseT or 1000BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An 802.11b, 802.11g, or 802.11n wireless card installed on each wireless station
- A broadband Internet connection via cable or DSL modem, with Ethernet (RJ-45)

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

Figure 6: Safe@Office 1000NW Appliance Rear Panel

The following table lists the Safe@Office 1000NW appliance's rear panel elements.

Table 10: Safe@Office 1000NW Appliance Rear Panel Elements

Label	Description
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
WAN	Wide Area Network switch: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the

Label	Description
	Internet.
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
USB	Two USB 2.0 ports used for connecting USB-based printers or modems
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (10 seconds or until the SYS LED begins to blink rapidly). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
ANT 1/ ANT 2	Antenna connectors, used to connect the supplied wireless antennas .

Front Panel

The Safe@Office 1000NW appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 7: Safe@Office 1000NW Appliance Front Panel

For an explanation of the Safe@Office 1000NW appliance's status LEDs, see the table below.

Table 11: Safe@Office 1000NW Appliance Status LEDs

LED	State	Explanation
Power	Off	Power off
	On (Green)	Normal operation
System	On (Red)	Boot failed or TFTP mode
	Flashing quickly (Red)	High temperature or system failure
	Flashing slowly (Orange)	Writing update to flash memory

	Flashing quickly (Green)	System boot in progress
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
Security	Off	Normal operation
	Flashing for 5 sec (Orange)	Virus blocked
	Flashing for 1 sec (Red)	Hacker attack blocked
GbE Status (WAN / DMZ / LAN 1-4)	1000Mbps Off, LINK/ACT Off	No Link
	1000Mbps Off, LINK/ACT On (Green)	10 Mbps link established for the corresponding port
	1000Mbps On (Orange), LINK/ACT On	100 Mbps link established for the corresponding port
	1000Mbps On (Green), LINK/ACT On	1000 Mbps link established for the corresponding port
	1000Mbps Off, LINK/ACT Flashing (Green)	10 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Orange), LINK/ACT Flashing (Green)	100 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Green), LINK/ACT Flashing (Green)	1000 Mbps link established for the corresponding port Data is being transmitted/received

VPN	Off	No VPN tunnel established
	On (Green)	VPN idle / No activity
	Flashing (Green)	VPN activity
RS232/Serial	Off	No data terminal connected
	On (Green)	Data terminal ready
	Flashing (Green)	Serial activity
WLAN	Off	WLAN not enabled/connected
	On (Green)	WLAN connected in idle / No activity
	Flashing (Green)	WLAN activity
USB	Off	No USB device connected
	On (Green)	USB device connected
	Flashing (Green)	Activity on the USB device

Getting to Know Your Safe@Office 1000NW ADSL Appliance

1000NW ADSL

Package Contents

The Safe@Office 1000NW ADSL package includes the following:

- Safe@Office 1000NW ADSL Wireless Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- Two antennas
- USB extension cable
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT or 1000BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An 802.11b, 802.11g, or 802.11n wireless card installed on each wireless station
- An ADSL line suitable for your appliance model:
    - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
    - For Annex B ADSL models, an ADSL over ISDN line (digital line)

- A splitter with a micro-filter, installed on all the jacks connected to the same phone line
- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

Figure 8: Safe@Office 1000NW ADSL Appliance Rear Panel

The following table lists the Safe@Office 1000NW ADSL appliance's rear panel elements.

Table 12: Safe@Office 1000NW ADSL Appliance Rear Panel Elements

Label	Description
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
USB	A USB 2.0 port used for connecting a USB-based printer or modem
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (10 seconds or until the SYS LED begins to blink rapidly). Resets the Safe@Office appliance to its factory defaults, and resets your

Label	Description
	firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
ANT 1/ ANT 2	Antenna connectors, used to connect the supplied wireless antennas .

Side Panel

The side panel includes a slot for inserting an ExpressCard cellular modem.

Figure 9: Safe@Office 1000NW ADSL Appliance Side Panel

Front Panel

The Safe@Office 1000NW ADSL appliance includes several status LEDs that enable you to monitor the appliance's operation.

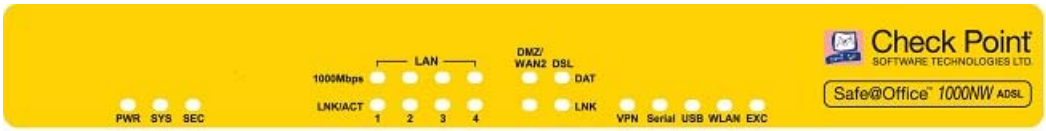


Figure 10: Safe@Office 1000NW ADSL Appliance Front Panel

For an explanation of the Safe@Office 1000NW ADSL appliance's status LEDs, see the table below.

Table 13: Safe@Office 1000NW ADSL Appliance Status LEDs

LED	State	Explanation
Power	Off	Power off
	On (Green)	Normal operation
System	On (Red)	Boot failed or TFTP mode
	Flashing quickly (Red)	High temperature or system failure
	Flashing slowly (Orange)	Writing update to flash memory
	Flashing quickly (Green)	System boot in progress
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
Security	Off	Normal operation
	Flashing for 5 sec (Orange)	Virus blocked
	Flashing for 1 sec (Red)	Hacker attack blocked

GbE Status (LAN 1-4 / DMZ/WAN2)	1000Mbps Off, LINK/ACT Off	No Link
	1000Mbps Off, LINK/ACT On (Green)	10 Mbps link established for the corresponding port
	1000Mbps On (Orange), LINK/ACT On	100 Mbps link established for the corresponding port
	1000Mbps On (Green), LINK/ACT On	1000 Mbps link established for the corresponding port
	1000Mbps Off, LINK/ACT Flashing (Green)	10 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Orange), LINK/ACT Flashing (Green)	100 Mbps link established for the corresponding port Data is being transmitted/received
	1000Mbps On (Green), LINK/ACT Flashing (Green)	1000 Mbps link established for the corresponding port Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received

VPN	Off	No VPN tunnel established
	On (Green)	VPN idle / No activity
	Flashing (Green)	VPN activity
RS232/Serial	Off	No data terminal connected
	On (Green)	Data terminal ready
	Flashing (Green)	Serial activity
USB	Off	No USB device connected
	On (Green)	USB device connected
	Flashing (Green)	Activity on the USB device
WLAN	Off	WLAN not enabled/connected
	On (Green)	WLAN connected in idle / No activity
	Flashing (Green)	WLAN activity
EXC	Off	No ExpressCard connected
	On (Green)	ExpressCard connected
	Flashing (Green)	Activity on the ExpressCard

Getting to Know Your Safe@Office 500 Appliance

500

Package Contents

The Safe@Office 500 package includes the following:

- Safe@Office 500 Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- RS232 serial adaptor (RJ45 to DB9); model SBX-166LHGE-5 only

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

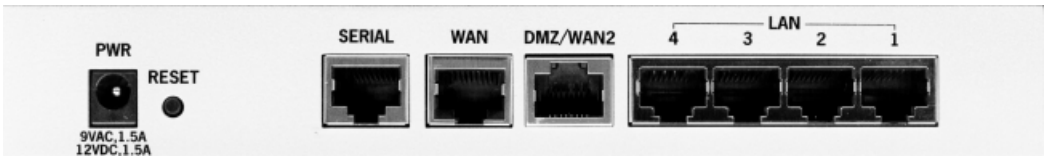


Figure 11: Safe@Office 500 SBX-166LHGE-5 Appliance Rear Panel

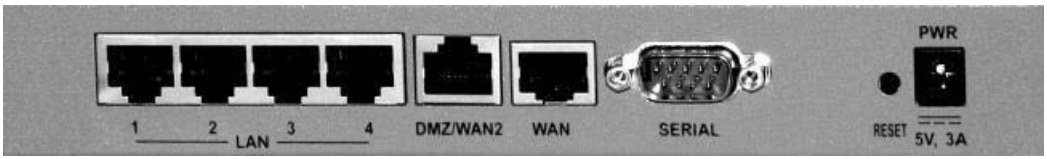


Figure 12: Safe@Office 500 SBX-166LHGE-6 Appliance Rear Panel

The following table lists the Safe@Office 500 appliance's rear panel elements.

Table 14: Safe@Office 500 Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. Depending on the appliance model, this port may have either a DB9 RS232 connector, or an RJ-45 connector. In models with an RJ-45 connector, an RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.

Label	Description
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the Internet.
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices.

Front Panel

The Safe@Office 500 appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 13: Safe@Office 500 Appliance Front Panel

For an explanation of the Safe@Office 500 appliance's status LEDs, see the following table.

Table 15: Safe@Office 500 Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection

LED	State	Explanation
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ WAN/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity

Getting to Know Your Safe@Office 500 ADSL Appliance

Package Contents

The Safe@Office 500 ADSL package includes the following:

- Safe@Office 500 ADSL Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- USB extension cable
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An ADSL line suitable for your appliance model:
  - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
  - For Annex B ADSL models, an ADSL over ISDN line (digital line)
- A splitter with a micro-filter, installed on all the jacks connected to the same phone line

- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

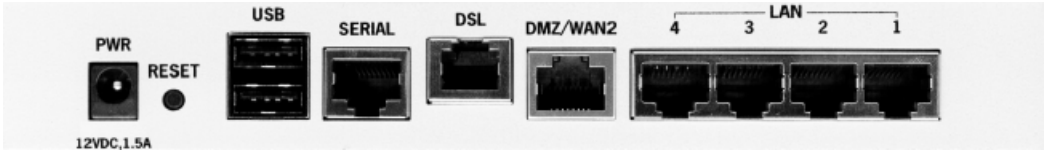


Figure 14: Safe@Office 500 ADSL Appliance Rear Panel

The following table lists the Safe@Office 500 ADSL appliance's rear panel elements.

Table 16: Safe@Office 500 ADSL Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
USB	Two USB 2.0 ports used for connecting USB-based printers or modems

Label	Description
Serial	An RJ-45 serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices.

Front Panel

The Safe@Office 500 ADSL appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 15: Safe@Office 500 ADSL Appliance Front Panel

For an explanation of the Safe@Office 500 ADSL appliance's status LEDs, see the following table.

Table 17: Safe@Office 500 ADSL Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port

LED	State	Explanation
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity

Getting to Know Your Safe@Office 500W Appliance

500W

Package Contents

The Safe@Office 500W package includes the following:

- Safe@Office 500W Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9); model SBXW-166LHGE-5 only
- Two antennas
- USB extension cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An 802.11b, 802.11g or 802.11 Super G wireless card installed on each wireless station
- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

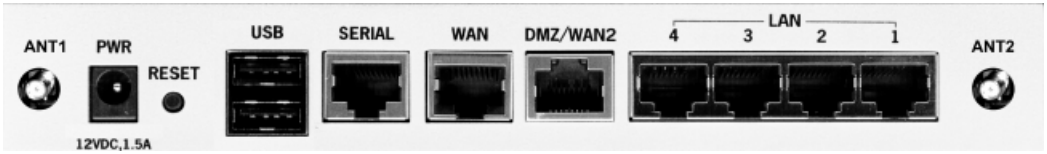


Figure 16: Safe@Office 500W SBXW-166LHGE-5 Appliance Rear Panel

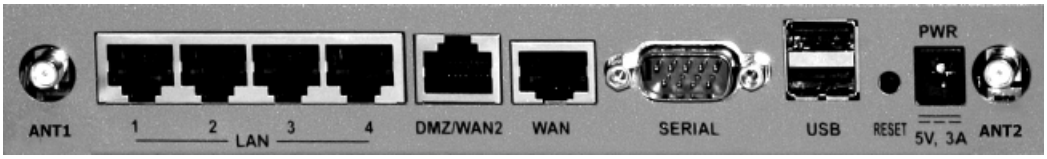


Figure 17: Safe@Office 500W SBXW-166LHGE-6 Appliance Rear Panel

The following table lists the Safe@Office 500W appliance's rear panel elements.

Table 18: Safe@Office 500W Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
USB	Two USB 2.0 ports used for connecting USB-based printers or modems
Serial	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. Depending on the appliance model, this port may have either a DB9 RS232 connector, or an RJ-45 connector. In models with an RJ-45 connector, an RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the Internet.
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.

Label	Description
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices.
ANT 1/ ANT 2	Antenna connectors, used to connect the supplied wireless antennas .

Front Panel

The Safe@Office 500W appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 18: Safe@Office 500W Appliance Front Panel

For an explanation of the Safe@Office 500W appliance's status LEDs, see the following table.

Table 19: Safe@Office 500W Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation

LED	State	Explanation
	On (Red)	Error
	Flashing (Orange)	Software update in progress
LAN 1-4/ WAN/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity
WLAN	Off	No WLAN activity
	Flashing (Green)	WLAN activity

Getting to Know Your Safe@Office 500W ADSL Appliance

500W ADSL

Package Contents

The Safe@Office 500W ADSL package includes the following:

- Safe@Office 500W ADSL Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- Two antennas
- USB extension cable
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An ADSL line suitable for your appliance model:
  - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
  - For Annex B ADSL models, an ADSL over ISDN line (digital line)
- A splitter with a micro-filter, installed on all the jacks connected to the same phone line

- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).
- An 802.11b, 802.11g or 802.11 Super G wireless card installed on each wireless station

Rear Panel

All physical connections (network and power) are made via the rear panel of your Safe@Office appliance.

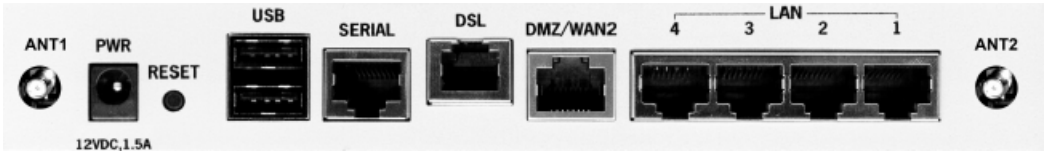


Figure 19: Safe@Office 500W ADSL Appliance Rear Panel

The following table lists the Safe@Office 500W ADSL appliance's rear panel elements.

Table 20: Safe@Office 500W ADSL Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
USB	Two USB 2.0 ports used for connecting USB-based printers or modems

Label	Description
Serial	An RJ-45 serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port or as a VLAN trunk.
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices.
ANT1 / ANT2	Antenna connectors, used to connect the supplied wireless antennas .

Front Panel

The Safe@Office 500W ADSL appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 20: Safe@Office 500W ADSL Appliance Front Panel

For an explanation of the Safe@Office 500W ADSL appliance's status LEDs, see the following table.

Table 21: Safe@Office 500W ADSL Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port

LED	State	Explanation
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity
WLAN	Off	No WLAN activity
	Flashing (Green)	WLAN activity

Contacting Technical Support

In case of a problem with your Safe@Office appliance, see http://www.sofaware.com/support.

You can also download the latest version of this guide from the site.

Chapter 2

Safe@Office Security

This chapter explains the basic security concepts on which Safe@Office security is based.

This chapter includes the following topics:

Introduction to Information Security 71
The Safe@Office Firewall 76

Introduction to Information Security

Network security is but a small part of information security, which in turn is only a fraction of general security. In order to understand why the Safe@Office appliance is the best product for securing the business network, we must first examine information security requirements in general.

Information is Valuable!

The most valuable asset an organization has is its information. The type of information maintained by an organization depends on the organization's type and purpose. For example:

- Almost every organization stores information about its operations, such as employees' names and other personal details, salaries, and so on.
- Depending on the role of different governmental offices, they may store personal information about citizens, residential addresses, car licenses registration, and so on.
- The army stores information about its soldiers, weapons inventory, and intelligence information about other armies. Much of this information is confidential.
- A bank stores information about its customers' accounts, their money transactions, ATM machine access codes, and so on. Much of this information is confidential.

- Commercial companies store information about their revenues, business and marketing plans, current and future product lines, information about competitors, and so on.

Just as the type of information may differ from organization to organization, the form in which it is stored may vary. For example, some forms of information are:

- Information recorded in written media, such as paper documents, books, and files
- Knowledge that is stored in a person's mind and can be exchanged verbally
- Information stored on electronic media, such as computers' hard drives, CDs, and tapes

The form in which an organization stores its information may make the information more or less accessible to people outside the organization.

Why Protect Business Information?

There are various reasons why it is necessary to protect business information:

- To prevent the theft, abuse, misuse, or any form of damage to crucial information

  For example, no business wants to find its customer list or future secret product line plans in the hands of the competition.

- To comply with local laws

  Local laws may enforce the protection, integrity, and availability of specific information, such as an individual's personal details, in order to respect the individual's right to privacy. Local laws may also enforce the security requirements made in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- To comply with another organization's security requirements

  Some organizations require their business partners to comply with international standards of security.

Information Security Challenges

The challenges of information security can be divided into the following areas:

- Confidentiality and Privacy - Ensuring that only the intended recipients can read certain information
- Authentication - Ensuring that information is actually sent by the stated sender
- Integrity - Ensuring that the original information was not altered and that no one tampered with it
- Availability - Ensuring that important information can be accessed at all times and places

The Security Policy

In order to meet these challenges, an organization must create and enforce a *security policy*. A security policy is a set of rules that defines how and by whom sensitive information should be accessed, handled, and distributed, both within and outside of the organization. For example, a security policy may include the following rules regarding visitors who arrive at an enterprise building's lobby:

- Visitors must sign in at the entrance desk.
- Visitors must wear a visitor badge and be escorted while in the building.
- Visitors cannot use their badge to open electronic doors.

Other types of security policy rules and measures might be:

- Only the executive manager has access to financial reports.
- Visitors must open their bags for a security check.
- Surveillance cameras should be positioned in the area of the building.
- Passwords must be changed on a daily basis.
- Confidential papers must be shredded after use.

An organization's security policy is usually designed by a person who is in charge of handling all security matters for the organization. This person is called a *security manager*.

In order for a security policy be effective, it must be accompanied by the following measures:

- Awareness - A security policy must be accompanied by steps taken to increase the employees' awareness of security issues. If employees are unaware of a security policy rule and the reason for it, they are likely to break it.
- Enforcement - To enforce a security policy, an organization can take various measures, both human and electronic. For example:
  - Installing surveillance cameras in strategic locations throughout the organization
  - Positioning human guards who have the authority to prevent other people from entering the premises or certain areas on the premises
  - Installing alarms that are triggered upon certain conditions
  - Using magnetic identification tags to enforce and log access permissions to different areas on the premises
  - Using “red phones” to encrypt highly confidential voice phone calls
- Updating - A security policy is a living thing that must be updated from time to time according to changing situations.

Unfortunately, even when a security policy is accompanied by these measures, its effectiveness is limited against a person with malicious intent.

Computer and Network Security

A great deal of an organization's existing information is processed and stored electronically by single (standalone) computers or computer networks. Therefore, an attack on an organization's computers or computer networks can result in extensive information theft or abuse. However, computers and computer networks today are not just tools used to store information; they are the heart of an organization's operations and crucial to its communication and business transactions. For example:

- Nowadays, most of an organization's communication and business transactions are conducted via email (regardless of the organization's size).
- Online stores process orders and supply products over the Internet.
- Emerging technology today allows an organization's branch offices to communicate, share data, and even establish low-cost VoIP (Voice over IP) communications, rather then using the traditional phone system.

- Applications are hosted on a main computer rather than on personal workstations. This helps organizations share application resources. For example, in service departments, the customer database is located on a main computer, while all customer relations transactions are managed by software clients running on the agents' computers.
- In order to withdraw money from any ATM machine, your PIN and the details on your magnetic card are scanned and verified against the details on the main bank computer.
- A department store in New York can query the inventory of the main warehouse located in Chicago and enter orders for missing products, all in real time.

In other words, on top of the damage done by computer information theft or abuse, unauthorized access to a computer or a computer network can seriously damage the entire organization's essential operations, communications, and productivity. For example:

- An online store's Web site can be hacked, so customers cannot enter orders.
- An unauthorized user can take advantage of an organization's email server to send unsolicited bulks of email. As a result, the organization's Internet communication lines will be overloaded, and employees in the organization will be unable to send or receive emails.

Since computer and network security has become a central part of information and general security, security managers must either have an understanding of computers and networking, or work closely with network administrators and network security specialists.

Network Security and the Small Business

Network security has been and continues to be a major concern for large, enterprise-sized organizations. However, small businesses are no less of a target for Internet attacks, and they require a similar network security level, for the following reasons:

- Small business owners lack awareness of network security and unwittingly leave the door open to threats from within the network. For example, peer-to-peer applications are a source of virus-infected files, Trojans, and worms, any of which can be used to steal confidential information such as credit card numbers; however, many small business owners are unaware of the risk, and therefore do not block their employees from using peer-to-peer applications.

- Large businesses have the funds and expertise to constantly enhance their security and are therefore a difficult target for hackers. This makes small businesses a far more attractive target for network attacks.
- The state's awareness of privacy and data protection is enforced through legislation. For example, the Health Insurance Portability and Accountability Act (HIPAA) that was enacted by the U.S. Congress in 1996 gives patients access to their medical files electronically, and therefore strictly defines the requirements for protecting electronic confidential data.

Not only are small businesses more vulnerable to Internet attacks, but due to their relative lack of technical and financial resources, they may suffer more damage than large organizations and the recovery may be more difficult.

The Safe@Office Firewall

What Is a Firewall?

The most effective way to secure an Internet link is to put a firewall between the local network and the Internet. A *firewall* is a system designed to prevent unauthorized access to or from a secured network. Firewalls act as locked doors between internal and external networks: data that meets certain requirements is allowed through, while unauthorized data is not.

To provide robust security, a firewall must track and control the flow of communication passing through it. To reach control decisions for TCP/IP-based services, (such as whether to accept, reject, authenticate, encrypt, and/or log communication attempts), a firewall must obtain, store, retrieve, and manipulate information derived from all communication layers and other applications.

Security Requirements

In order to make control decisions for new communication attempts, it is not sufficient for the firewall to examine packets in isolation. Depending upon the communication attempt, both the communication state (derived from past communications) and the application state (derived from other applications) may be critical in the control decision. Thus, to ensure the highest level of security, a firewall must be capable of accessing, analyzing, and utilizing the following:

- Communication information - Information from all seven layers in the packet
- Communication-derived state - The state derived from previous communications. For example, the outgoing PORT command of an FTP session could be saved so that an incoming FTP data connection can be verified against it.
- Application-derived state - The state information derived from other applications. For example, a previously authenticated user would be allowed access through the firewall for authorized services only.
- Information manipulation - The ability to perform logical or arithmetic functions on data in any part of the packet. For example, the ability to encrypt packets.

Old Firewall Technologies

Older firewall technologies, such as packet filtering and application-layer gateways, are still in use in some environments. It is important to familiarize yourself with these technologies, so as to better understand the benefits and advantages of the Check Point Stateful Inspection firewall technology.

Packet Filters

Historically implemented on routers, packet filters filter user-defined content, such as IP addresses. They examine a packet at the network or transport layer and are application-independent, which allows them to deliver good performance and scalability.

Packet filters are the least secure type of firewall, as they are not application-aware, meaning that they cannot understand the context of a given communication. This makes them relatively easy targets for unauthorized entry to a network. A limitation of this type of filtering is its inability to provide security for basic protocols.

Packet filters have the following advantages and disadvantages:

Table 22: Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

Application-Layer Gateways

Application-layer gateways improve security by examining all application layers, bringing context information into the decision-making process. However, the method they use to do this disrupts the client/server model, reducing scalability. Ordinarily, a client sends requests for information or action according to a specific protocol, and the server responds, all in one connection. With application-layer gateways, each client/server communications requires two connections: one from a client to a proxy, and one from a proxy to a server. In addition, each proxy requires a different process (or daemon), making support for new applications a problem.

Application-layer gateways have the following advantages and disadvantages:

Table 23: Application-Layer Gateway Advantages and Disadvantages

Advantages	Disadvantages
Good security	Poor performance
Full application-layer awareness	Limited application support
	Poor scalability (breaks the client/server model)

Check Point Stateful Inspection Technology

Invented by Check Point, Stateful Inspection is the industry standard for network security solutions. A powerful inspection module examines every packet, ensuring that packets do not enter a network unless they comply with the network's security policy.

Stateful Inspection technology implements all necessary firewall capabilities between the data and network layers. Packets are intercepted at the network layer for best performance (as in packet filters), but the data derived from layers 3-7 is accessed and analyzed for improved security (compared to layers 4-7 in application-layer gateways). Stateful Inspection incorporates communication and application-derived state and context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. Stateful Inspection also delivers the ability to create virtual-session information for tracking connectionless protocols, such as UDP-based and RPC applications.

Safe@Office appliances use Stateful Inspection technology to analyze all packet communication layers and extract the relevant communication and application state information. The Safe@Office appliance is installed at the entry point to your network, and serves as the gateway for the internal network computers. In this ideal location, the inspection module can inspect all traffic before it reaches the network.

Packet State and Context Information

To track and act on both state and context information for an application is to treat that traffic *statefully*. The following are examples of state and context-related information that a firewall should track and analyze:

- Packet-header information (source and destination address, protocol, source and destination port, and packet length)
- Connection state information (which ports are being opened for which connection)
- TCP and IP fragmentation data (including fragments and sequence numbers)
- Packet reassembly, application type, and context verification (to verify that the packet belongs to the communication session)
- Packet arrival and departure interface on the firewall
- Layer 2 information (such as VLAN ID and MAC address)
- Date and time of packet arrival or departure

The Safe@Office firewall examines IP addresses, port numbers, and any other information required. It understands the internal structures of the IP protocol family and applications, and is able to extract data from a packet's application content and store it, to provide context in cases where the application does not provide it. The Safe@Office firewall also stores and updates the state and context information in dynamic tables, providing cumulative data against which it inspects subsequent communications.

The Stateful Inspection Advantage - Passive FTP Example

In order to discuss the strength of Stateful Inspection technology in comparison to the other firewall technologies mentioned, we will examine the Passive FTP protocol and the ways that firewalls handle Passive FTP traffic pass-through.

FTP connections are unique, since they are established using two sessions or channels: one for command (AKA control) and one for data. The following table describes the steps of establishing a Passive FTP connection, where:

- C is the client port used in the command session,
- D is the client port used in the data session, and
- P is the server port used in the data session.

Table 24: Establishment of Passive FTP Connection

Step	Channel Type	Description	Source	TCP Source Port	Destination	TCP Destination Port
1	CMD	Client initiates a PASV command to the FTP server on port 21	FTP client	C > 1023	FTP server	21
2	CMD	Server responds with data port information P > 1023	FTP server	21	FTP client	C

Step	Channel Type	Description	Source	TCP Source Port	Destination	TCP Destination Port
3	Data	Client initiates data connection to server on port P	FTP client	D > 1023	FTP server	P
4	Data	Server acknowledges data connection	FTP server	P	FTP client	D

The following diagram demonstrates the establishment of a Passive FTP connection through a firewall protecting the FTP server.

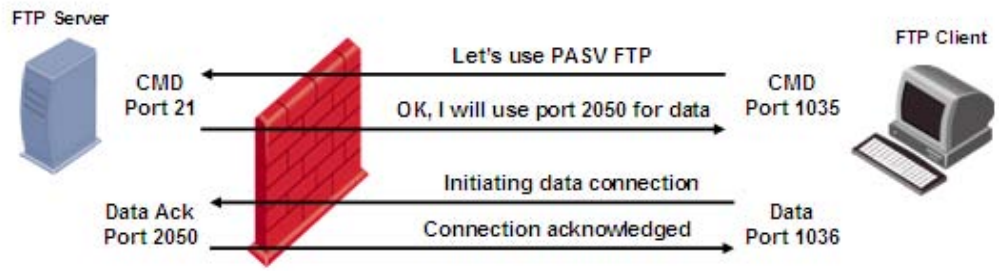


Figure 21: Establishment of Passive FTP Connection

From the FTP server's perspective, the following connections are established:

- Command connection from the client on a port greater than 1023, to the server on port 21
- Data connection from the client on a port greater than 1023, to the server *on a port greater than 1023*

The fact that both of the channels are established by the client presents a challenge for the firewall protecting the FTP server: while a firewall can easily be configured to identify incoming command connections over the default port 21, it must also be able to handle incoming data connections over a dynamic port that is negotiated randomly as part of the

FTP client-server communication. The following table examines how different firewall technologies handle this challenge:

Table 25: Firewall Technologies and Passive FTP Connections

Firewall Technology	Action
Packet Filter	Packet filters can handle outbound FTP connections in either of the following ways: • By leaving the entire upper range of ports (greater than 1023) open. While this allows the file transfer session to take place over the dynamically allocated port, it also exposes the internal network. • By shutting down the entire upper range of ports. While this secures the internal network, it also blocks other services. Thus packet filters' handling of Passive FTP comes at the expense of either application support or security.
Application-Layer Gateway (Proxy)	Application-layer gateways use an FTP proxy that acts as a go-between for all client-server sessions. This approach overcomes the limitations of packet filtering by bringing application-layer awareness to the decision process; however, it also takes a high toll on performance. In addition, each service requires its own proxy (an FTP proxy for FTP sessions, an HTTP proxy for HTTP session, and so on), and since the application-layer gateway can only support a certain number of proxies, its usefulness and scalability is limited. Finally, this approach exposes the operating system to external threats.

Firewall Technology	Action
Stateful Inspection Firewall	A Stateful Inspection firewall examines the FTP application-layer data in an FTP session. When the client initiates a command session, the firewall extracts the port number from the request. The firewall then records both the client and server's IP addresses and port numbers in an FTP-data pending request list. When the client later attempts to initiate a data connection, the firewall compares the connection request's parameters (ports and IP addresses) to the information in the FTP-data pending request list, to determine whether the connection attempt is legitimate. Since the FTP-data pending request list is dynamic, the firewall can ensure that only the required FTP ports open. When the session is closed, the firewall immediately closes the ports, guaranteeing the FTP server's continued security.

What Other Stateful Inspection Firewalls Cannot Do

The level of security that a stateful firewall provides is determined by the richness of data tracked, and how thoroughly the data is analyzed. Treating traffic statefully requires application awareness. Firewalls without application awareness must open a range of ports for certain applications, which leads to exploitable holes in the firewall and violates security “best practices”.

TCP packet reassembly on all services and applications is a fundamental requirement for any Stateful Inspection firewall. Without this capability, fragmented packets of legitimate connections may be dropped, or those carrying network attacks may be allowed to enter a network. The implications in either case are potentially severe. When a truly stateful firewall receives fragmented packets, the packets are reassembled into their original form. The entire stream of data is analyzed for conformity to protocol definition and for packet-payload validity.

True Stateful Inspection means tracking the state and context of all communications. This requires a detailed level of application awareness. The Safe@Office appliance provides true Stateful Inspection.

Chapter 3

Installing and Setting Up Safe@Office

This chapter describes how to properly set up and install your Safe@Office appliance in your networking environment.

This chapter includes the following topics:

Before You Install the Safe@Office Appliance 85
Appliance Installation.....99
Wall Mounting the Safe@Office Appliance.....103
Securing the Safe@Office Appliance against Theft.....105
Setting Up the Safe@Office Appliance.....107

Before You Install the Safe@Office Appliance

Prior to connecting and setting up your Safe@Office appliance for operation, you must do the following:

- Check if TCP/IP Protocol is installed on your computer.
- Check your computer's TCP/IP settings to make sure it obtains its IP address automatically.

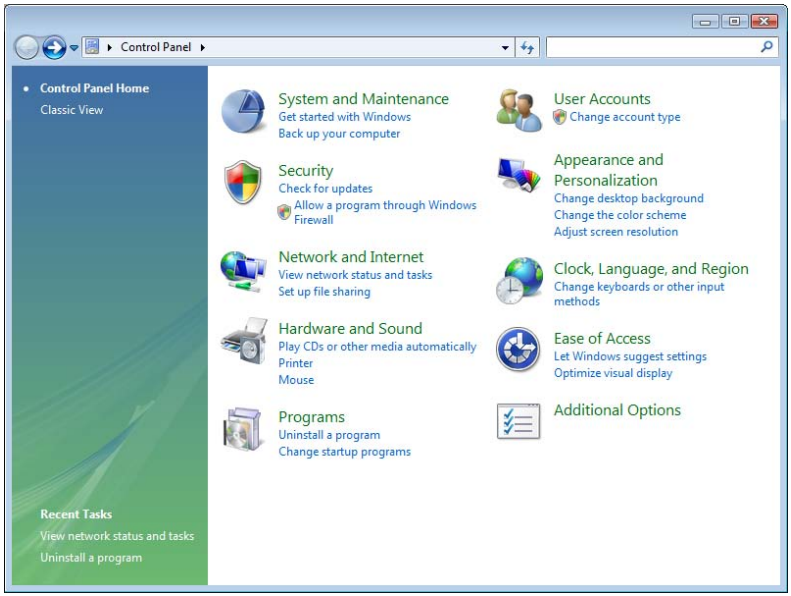
Refer to the relevant section in this guide in accordance with the operating system that runs on your computer. The sections below will guide you through the TCP/IP setup and installation process.

Windows Vista

Checking the TCP/IP Installation

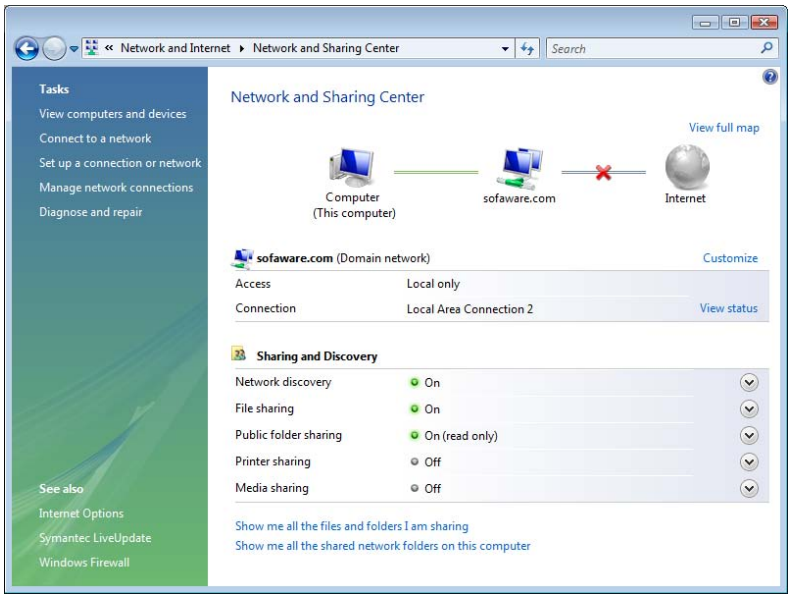
1. Click Start > Control Panel.

   The Control Panel window appears.



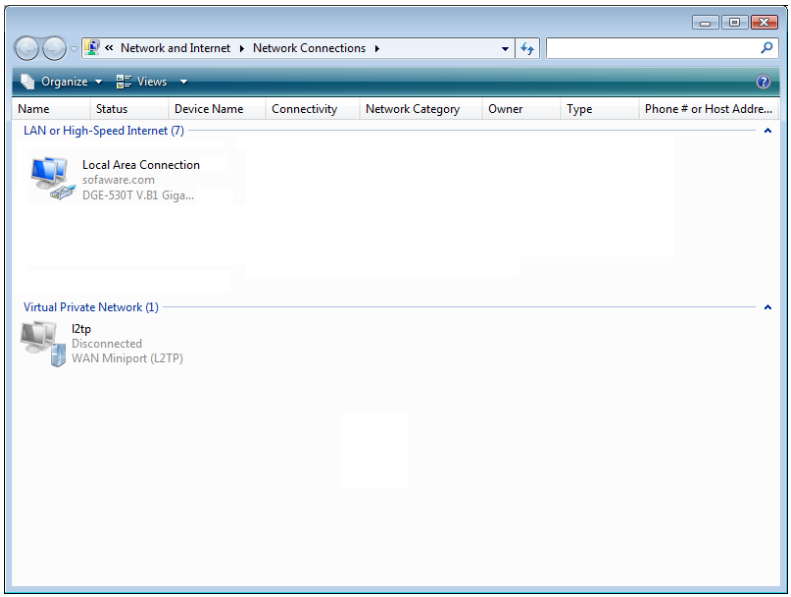
2. Under Network and Internet, click View network status and tasks.

The Network Sharing Center screen appears.



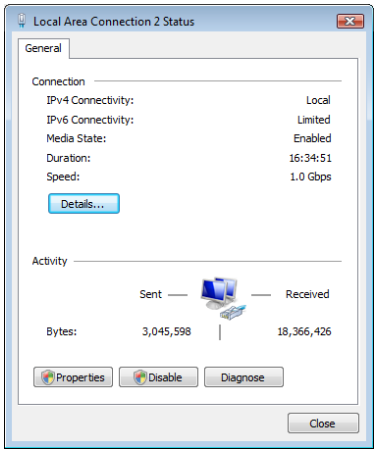
3. In the Tasks pane, click Manage network connections.

The Network Connections screen appears.



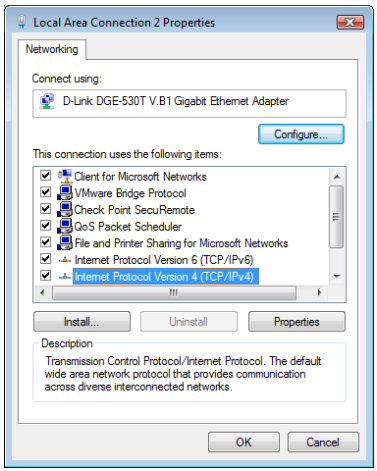
4. Double-click the Local Area Connection icon.

   The Local Area Connection Status window opens.



5. Click Properties.

The Local Area Connection Properties window opens.

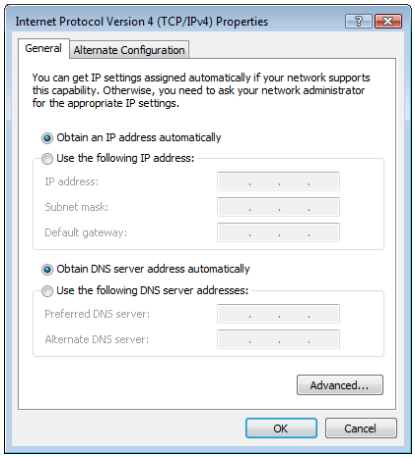


6. Check if Internet Protocol Version 4 (TCP/IPv4) appears in the list box and if it is properly configured with the Ethernet card installed on your computer.

TCP/IP Settings

1. In the Local Area Connection Properties window, double-click the Internet Protocol Version 4 (TCP/IPv4) component, or select it and click Properties.

   The Internet Protocol Version 4 (TCP/IPv4) Properties window appears.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2. Click the Obtain an IP address automatically radio button.

Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

(Note that 192.168.10 is the default value, and it may vary if you changed it in the Network > My Network page.)

3. Click the Obtain DNS server address automatically radio button.
4. Click OK to save the new settings.

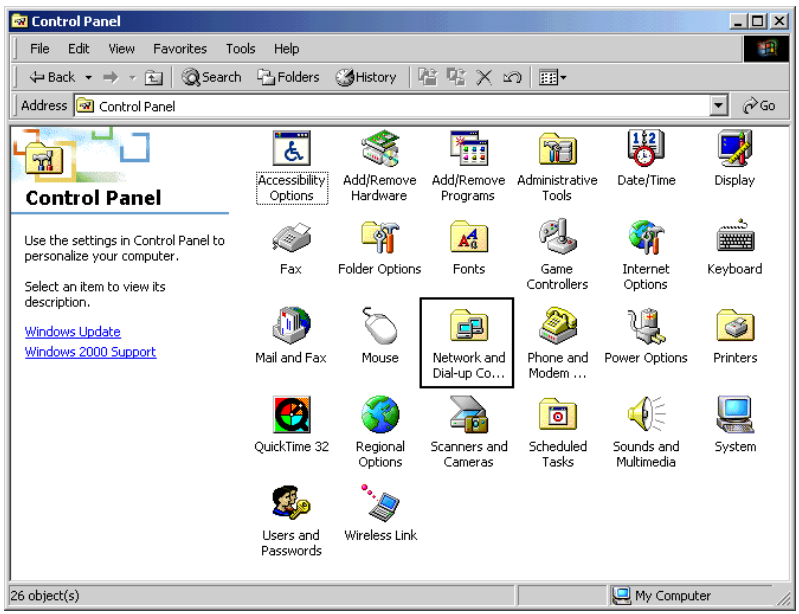
   Your computer is now ready to access your Safe@Office appliance.

Windows 2000/XP

Checking the TCP/IP Installation

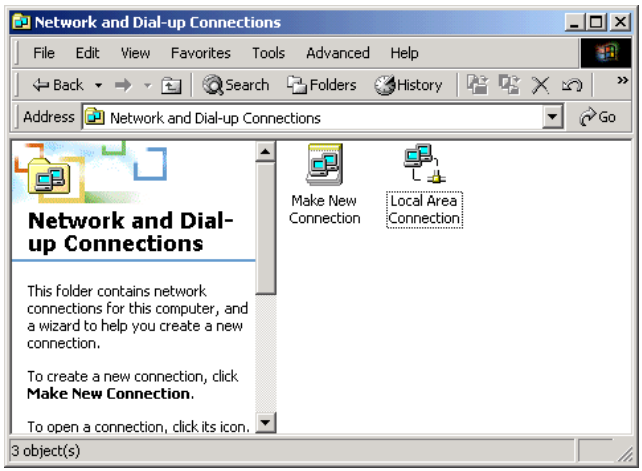
1. Click Start > Settings > Control Panel.

   The Control Panel window appears.



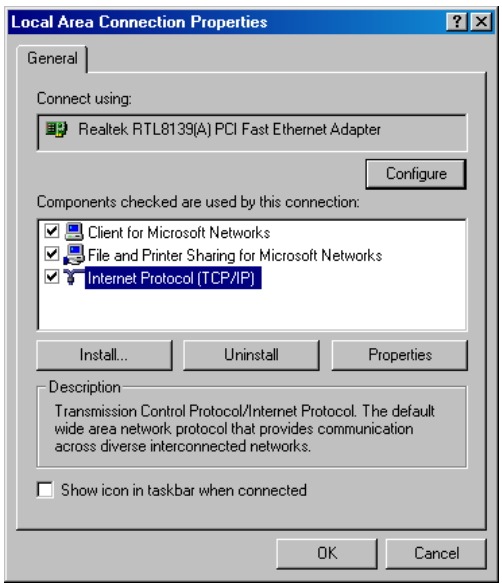
2. Double-click the Network and Dial-up Connections icon.

The Network and Dial-up Connections window appears.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
Network and Dial-up Connections
This folder contains network connections for this computer, and a wizard to help you create a new connection.
To create a new connection, click Make New Connection.
To open a connection, click its icon.
3 object(s)

3. Right-click the Local Area Connection icon and select Properties from the pop-up menu that opens.

   The Local Area Connection Properties window appears.

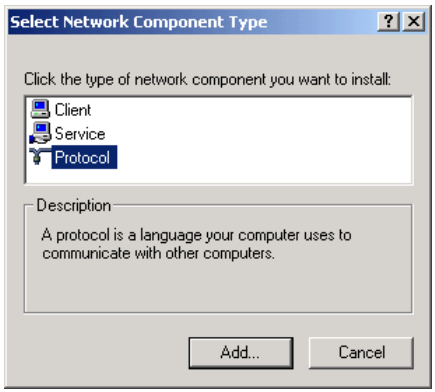


4. In the above window, check if TCP/IP appears in the components list and if it is properly configured with the Ethernet card installed on your computer. If TCP/IP does not appear in the Components list, you must install it as described in the next section.

Installing TCP/IP Protocol

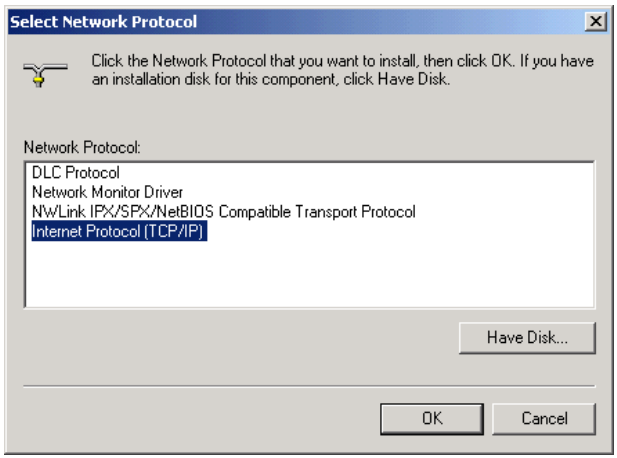
1. In the Local Area Connection Properties window click Install.

   The Select Network Component Type window appears.



2. Select Protocol and click Add.

   The Select Network Protocol window appears.


Select Network Protocol
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
Network Protocol:
DLC Protocol
Network Monitor Driver
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Internet Protocol (TCP/IP)
Have Disk...
OK
Cancel

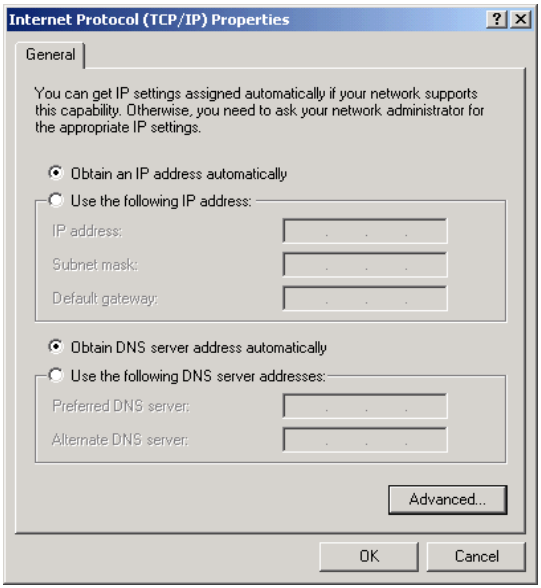
3. Choose Internet Protocol (TCP/IP) and click OK.

   TCP/IP protocol is installed on your computer.

TCP/IP Settings

1. In the Local Area Connection Properties window, double-click the Internet Protocol (TCP/IP) component, or select it and click Properties.

   The Internet Protocol (TCP/IP) Properties window opens.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2. Click the Obtain an IP address automatically radio button.

Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

(Note that 192.168.10 is the default value, and it may vary if you changed it in the Network > My Network page.)

3. Click the Obtain DNS server address automatically radio button.
4. Click OK to save the new settings.

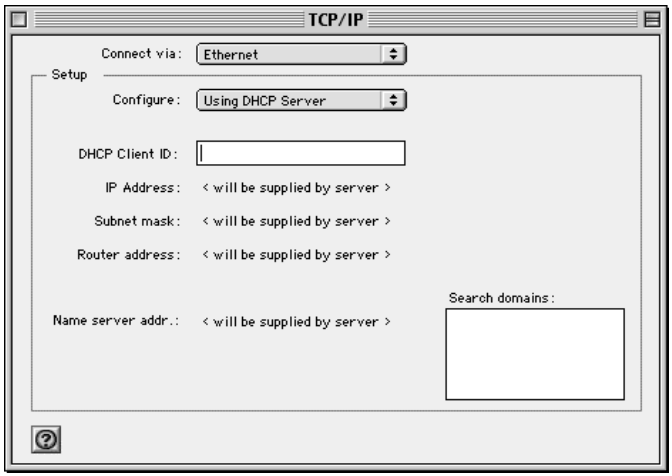
   Your computer is now ready to access your Safe@Office appliance.

Mac OS

Use the following procedure for setting up the TCP/IP Protocol.

1. Choose Apple Menus -> Control Panels -> TCP/IP.

   The TCP/IP window appears.



2. Click the Connect via drop-down list, and select Ethernet.
3. Click the Configure drop-down list, and select Using DHCP Server.
4. Close the window and save the setup.

Mac OS-X

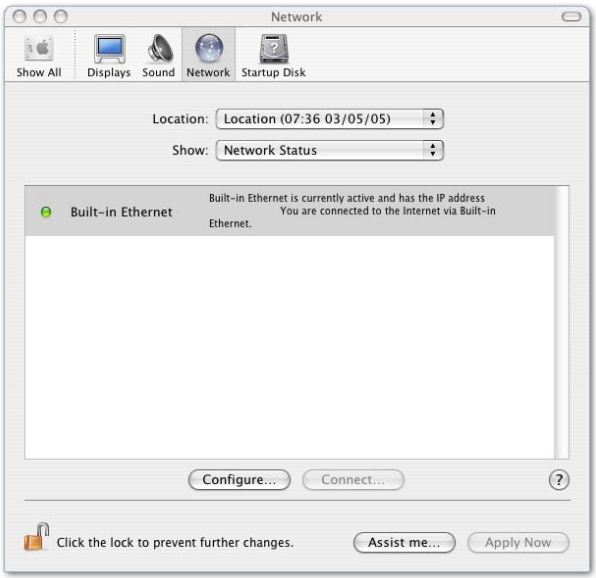
Use the following procedure for setting up the TCP/IP Protocol.

1. Choose Apple -> System Preferences.

   The System Preferences window appears.

2. Click Network.

The **Network** window appears.



3. Click **Configure.**

TCP/IP configuration fields appear.

4. Click the Configure IPv4 drop-down list, and select Using DHCP.
5. Click Apply Now.

Appliance Installation

Installing Non-ADSL Models

To install the Safe@Office appliance

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 61.

2. Connect the LAN cable:

   a. Connect one end of the Ethernet cable to one of the appliance's LAN ports.

   b. Connect the other end to PCs, hubs, or other network devices.

3. Connect the WAN cable:

   a) Connect one end of an Ethernet cable to the appliance's Ethernet WAN port.

   a. Connect the other end of the cable to a cable modem, DSL modem, or office network.

4. Connect the power adapter to the appliance's power socket, labeled PWR.

5. Plug the power adapter into the wall electrical outlet.

Warning: The Safe@Office appliance power adapter is compatible with either 100, 120 or 230 VAC input power. Verify that the wall outlet voltage is compatible with the voltage specified on your power adapter. Failure to observe this warning may result in injuries or damage to equipment.

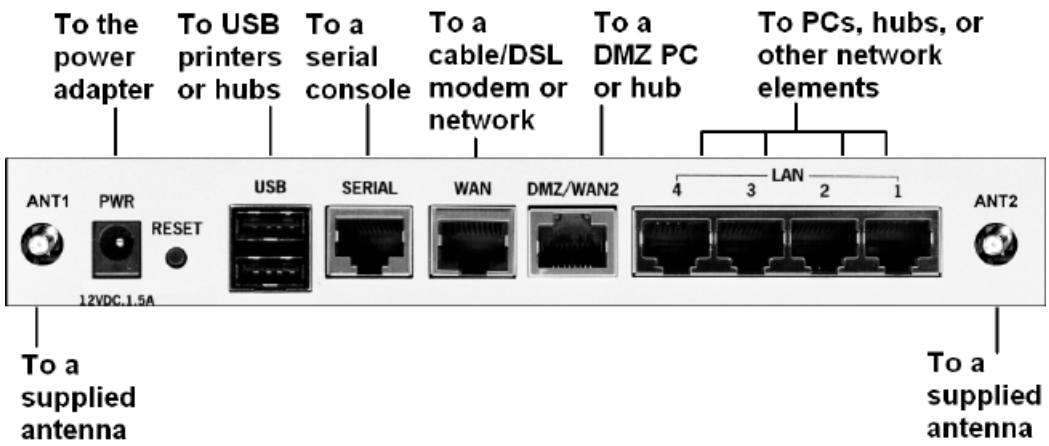


Figure 22: Typical Connection Diagram

Installing ADSL Models

ADSL

To install the Safe@Office appliance

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 61.

2. Connect the LAN cable:

   a. Connect one end of the Ethernet cable to one of the appliance's LAN ports.

   b. Connect the other end to PCs, hubs, or other network devices.

3. Connect the ADSL cable:

   a. Connect one end of the telephone cable to the appliance's DSL port.

   b. Connect the other end of the cable to the ADSL line or micro-filter.

   In most cases, a micro-filter is required for each phone jack on your line. The micro-filter prevents the standard phone lines from interfering with your ADSL service. Check with your service provider whether a micro-filter is required at your location.

4. To use the appliance with a non-ADSL connection, or with an existing ADSL modem, connect an Ethernet cable:
   a. Connect one end of the Ethernet cable to the appliance's DMZ/WAN2 port.
   b. Connect the other end of the cable to an external cable modem, DSL modem, or office network.
5. Connect the power adapter to the appliance's power socket, labeled PWR.
6. Plug the power adapter into the wall electrical outlet.

Warning: The Safe@Office appliance power adapter is compatible with either 100, 120 or 230 VAC input power. Verify that the wall outlet voltage is compatible with the voltage specified on your power adapter. Failure to observe this warning may result in injuries or damage to equipment.

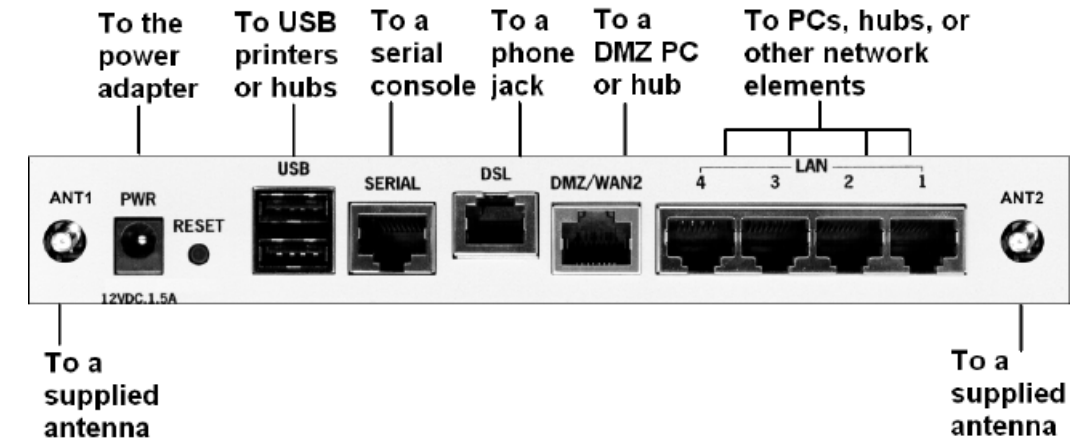


Figure 23: Typical Connection Diagram

Cascading Your Appliance

500 1000N

The Safe@Office appliance protects all computers and network devices that are connected to its LAN and DMZ ports. If desired, you can increase the appliance's port capacity by cascading hubs or switches.

To cascade the Safe@Office appliance to a hub or switch

1. Connect a standard Ethernet cable to one of the appliance's LAN ports or to its DMZ/WAN2 Ethernet port.

   The Safe@Office appliance automatically detects cable types, so you can use either a straight-through or crossed Ethernet cable.

2. Connect the other end of the cable to an Ethernet hub or switch.
3. Connect additional computers and network devices to the hub or switch as desired.

Preparing the Appliance for a Wireless Connection

500W 1000NW

To prepare the Safe@Office wireless appliance for a wireless connection

1. Connect the antennas that came with your Safe@Office wireless appliance to the antenna connectors in the appliance's rear panel.
2. Bend the antennas at the hinges, so that they point upwards.

Connecting the Appliance to Network Printers

USB

In models with a print server, you can connect network printers.

To connect network printers

1. Connect one end of a USB cable to one of the appliance's USB ports.

   If needed, you can use the provided USB extension cord.

2. Connect the other end to a printer or a USB 2.0 hub.

Warning: Verify that the USB devices' power requirement does not exceed the appliance's USB power adapter capabilities. Failure to observe this warning may cause damage to the appliance and void the warranty.

For information on setting up network printers, see ***Setting up Network Printers*** on page 768.

Wall Mounting the Safe@Office Appliance

500 1000N

For your convenience, the Safe@Office appliance includes a wall mounting kit, which consists of two plastic conical anchors and two cross-head screws.

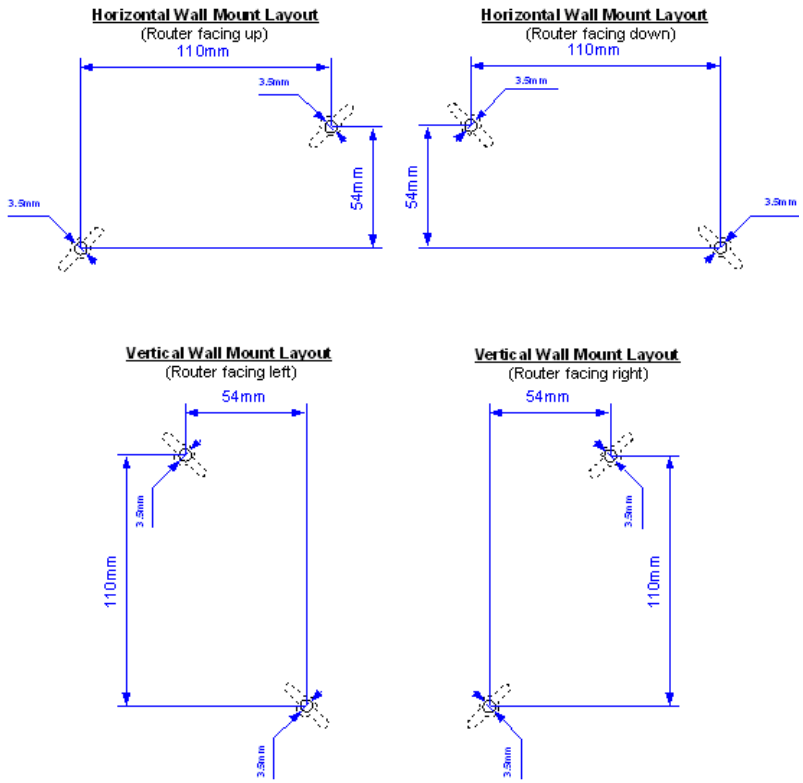
To mount the Safe@Office appliance on the wall

1. Decide where you want to mount your Safe@Office appliance.
2. Decide on the mounting orientation.

   You can mount the appliance on the wall facing up, down, left, or right.

Note: Mounting the appliance with the ports facing upwards is not recommended, as dust might accumulate in unused ports.

3. Mark two drill holes on the wall, in accordance with the following sketch:



4. Drill two 3.5 mm diameter holes, approximately 25 mm deep.
5. Insert two plastic conical anchors into the holes.

Note: The conical anchors you received with your Safe@Office appliance are suitable for concrete walls. If you want to mount the appliance on a plaster wall, you must use anchors that are suitable for plaster walls.

6. Insert the two screws you received with your Safe@Office appliance into the plastic conical anchors, and turn them until they protrude approximately 5 mm from the wall.
7. Align the holes on the Safe@Office appliance's underside with the screws on the wall, then push the appliance in and down.

Your Safe@Office appliance is wall mounted. You can now connect it to your computer.

Securing the Safe@Office Appliance against Theft

500 1000N

The Safe@Office appliance features a security slot to the rear of the right panel, which enables you to secure your appliance against theft, using an anti-theft security device.

Note: Anti-theft security devices are available at most computer hardware stores.

This procedure explains how to install a looped security cable on your appliance. A looped security cable typically includes the parts shown in the diagram below.

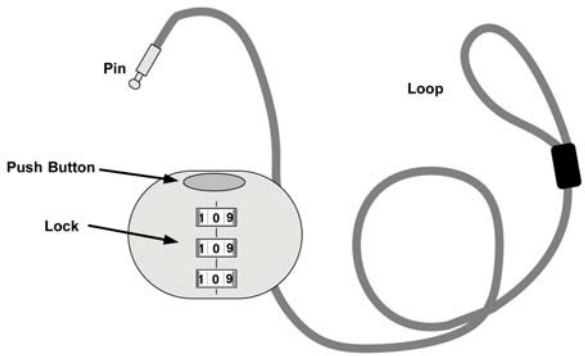


Figure 24: Looped Security Cable

While these parts may differ between devices, all looped security cables include a bolt with knobs, as shown in the diagram below:

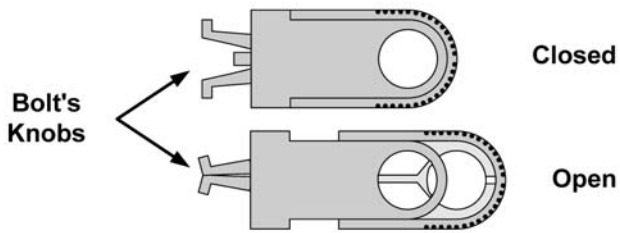
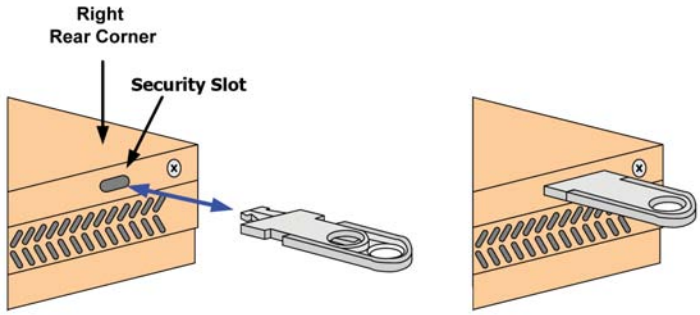


Figure 25: Looped Security Cable Bolt

The bolt has two states, Open and Closed, and is used to connect the looped security cable to the appliance's security slot.

To install an anti-theft device on the Safe@Office appliance

1. If your anti-theft device has a combination lock, set the desired code, as described in the documentation that came with your device.
2. Connect the anti-theft device's loop to any sturdy mounting point, as described in the documentation that came with your device.
3. Slide the anti-theft device's bolt to the Open position.
4. Insert the bolt into the Safe@Office appliance's security slot, then slide the bolt to the Closed position until the bolts holes are aligned.



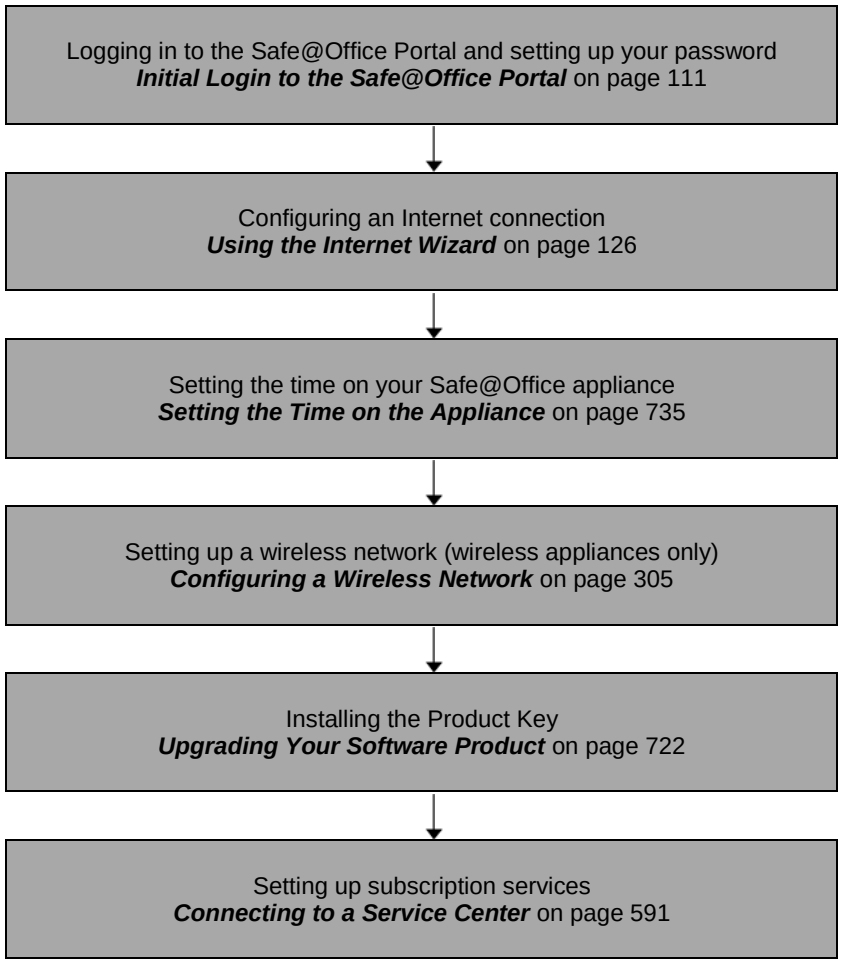
5. Thread the anti-theft device's pin through the bolt’s holes, and insert the pin into the main body of the anti-theft device, as described in the documentation that came with your device.

Setting Up the Safe@Office Appliance

500 1000N

After you have installed the Safe@Office appliance, you must set it up using the steps shown below.

When setting up your Safe@Office appliance for the first time after installation, these steps follow each other automatically. After you have logged in and set up your password, the Safe@Office Setup Wizard automatically opens and displays the dialog boxes for performing the initial configuration of the router. If desired, you can exit the Setup Wizard and perform each of these steps separately.

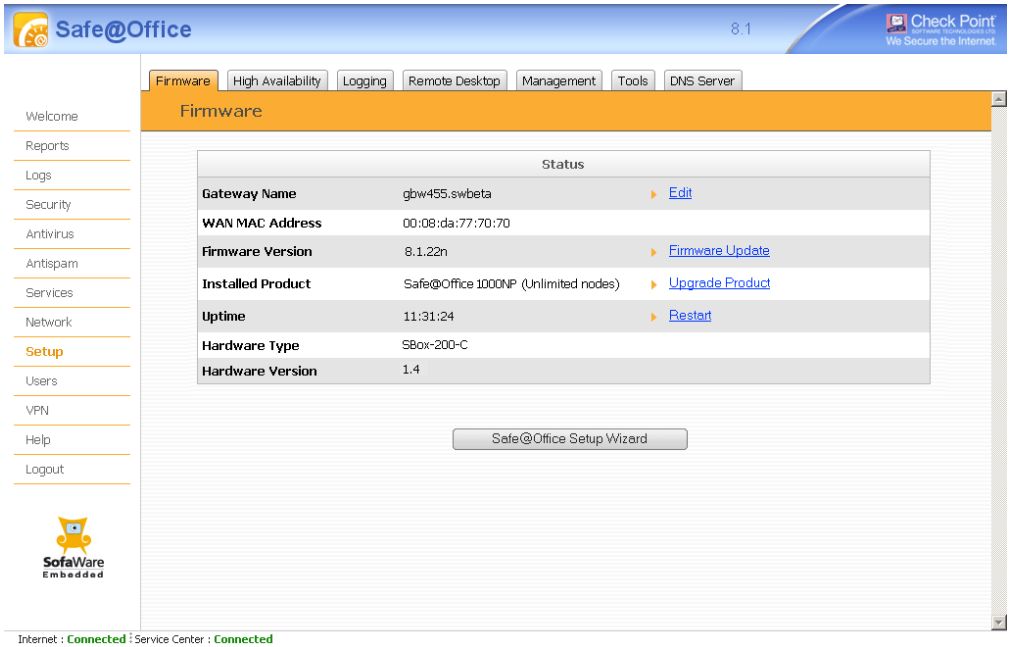

Logging in to the Safe@Office Portal and setting up your password
Initial Login to the Safe@Office Portal on page 111
Configuring an Internet connection
Using the Internet Wizard on page 126
Setting the time on your Safe@Office appliance
Setting the Time on the Appliance on page 735
Setting up a wireless network (wireless appliances only)
Configuring a Wireless Network on page 305
Installing the Product Key
Upgrading Your Software Product on page 722
Setting up subscription services
Connecting to a Service Center on page 591

You can access the Setup Wizard at any time after initial setup, using the procedure below.

To access the Setup Wizard

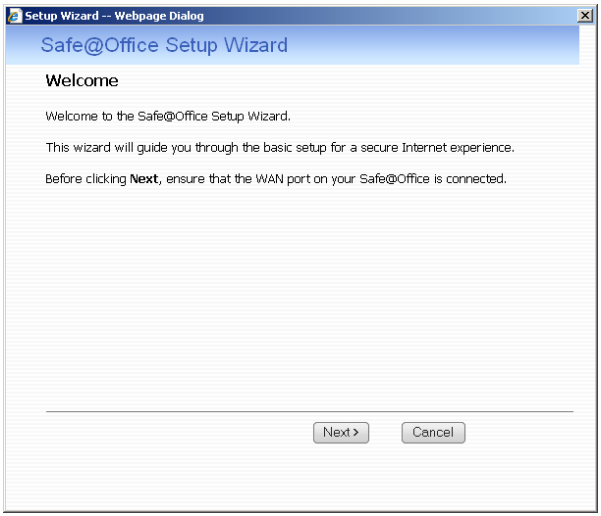
1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.



2. Click Safe@Office Setup Wizard.

The **Safe@Office Setup Wizard** opens with the **Welcome** page displayed.


Setup Wizard -- Webpage Dialog
Safe@Office Setup Wizard
Welcome
Welcome to the Safe@Office Setup Wizard.
This wizard will guide you through the basic setup for a secure Internet experience.
Before clicking Next, ensure that the WAN port on your Safe@Office is connected.
Next >
Cancel

Chapter 4

Getting Started

This chapter contains all the information you need in order to get started using your Safe@Office appliance.

This chapter includes the following topics:

Initial Login to the Safe@Office Portal.....111
Logging in to the Safe@Office Portal.....114
Accessing the Safe@Office Portal Remotely Using HTTPS 116
Using the Safe@Office Portal 118
Logging Out 123

Initial Login to the Safe@Office Portal

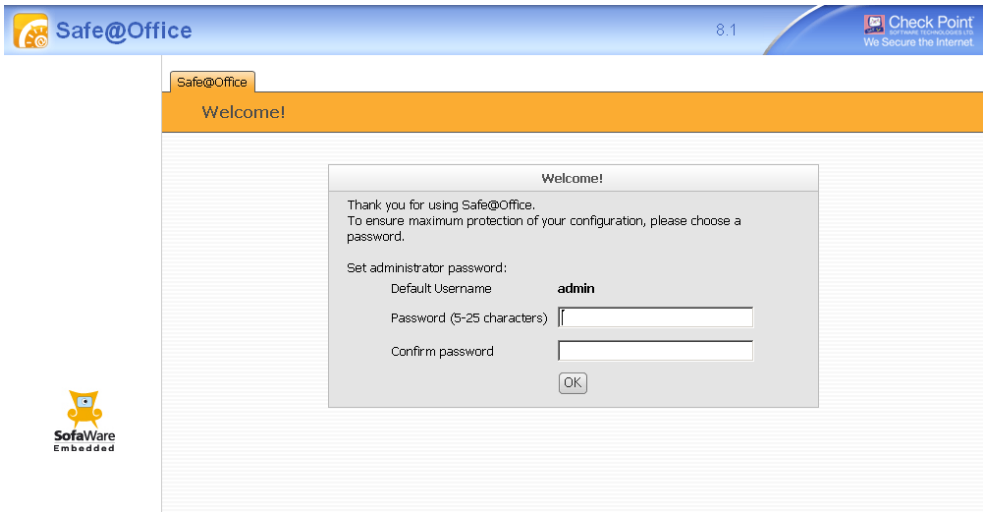
500 1000N

The first time you log in to the Safe@Office Portal, you must set up your password.

To log in to the Safe@Office Portal for the first time

1. Browse to http://my.firewall.

The initial login page appears.



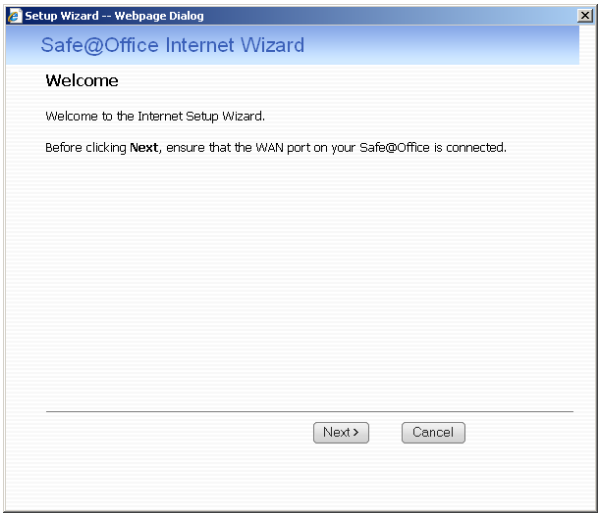
2. Type a password both in the **Password** and the **Confirm password** fields.

Note: The password must be five to 25 characters (letters or numbers).

Note: You can change your username and password at any time. For further information, see ***Changing Your Password*** on page *677*.

3. Click **OK**.

The Safe@Office Setup Wizard opens, with the Welcome page displayed.


Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Welcome
Welcome to the Internet Setup Wizard.
Before clicking Next, ensure that the WAN port on your Safe@Office is connected.
Next >
Cancel

4. Configure your Internet connection using one of the following ways:

   - Internet Wizard

     The Internet Wizard is the first part of the Setup Wizard, and it takes you through basic Internet connection setup, step by step. For information on using the Internet Wizard, see ***Using the Internet Wizard*** on page 126.

     After you have completed the Internet Wizard, the Setup Wizard continues to guide you through appliance setup. For more information, see ***Setting Up the Safe@Office Appliance*** on page 107.

   - Internet Setup

     Internet Setup offers advanced setup options, such as configuring two Internet connections. To use Internet Setup, click Cancel and refer to ***Using Internet Setup*** on page 141.

Logging in to the Safe@Office Portal

500 1000N

Note: By default, HTTP and HTTPS access to the Safe@Office Portal is not allowed from the WLAN, unless you do one of the following:

- Configure a specific firewall rule to allow access from the WLAN. See ***Using Rules*** on page 400.

  Or

- Enable HTTPS access from the Internet. See ***Configuring HTTPS*** on page 728.

To log in to the Safe@Office Portal

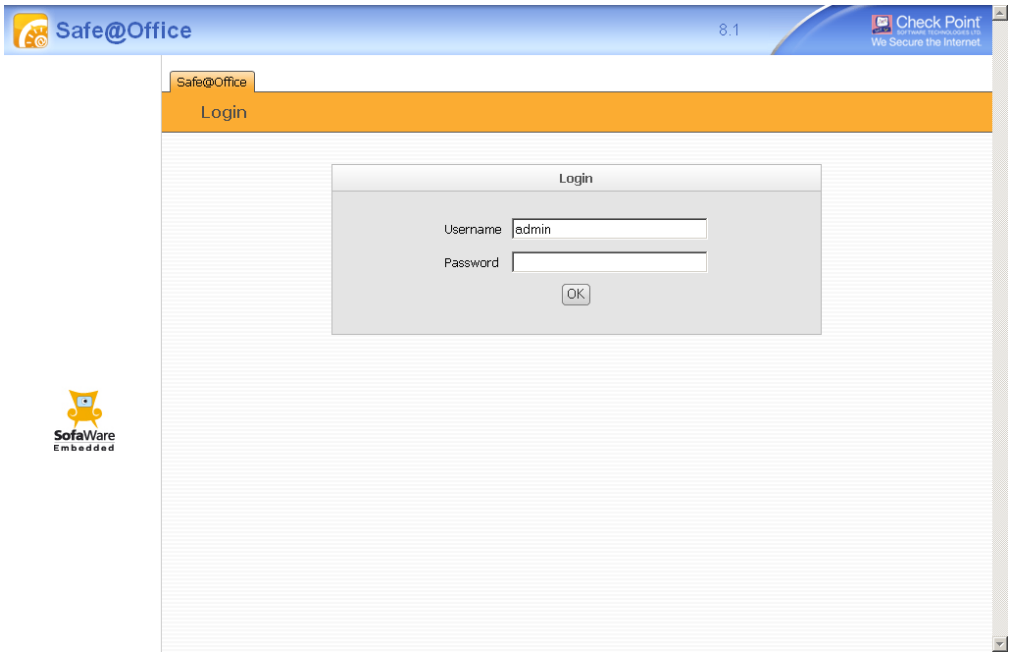
1. Do one of the following:

   - Browse to http://my.firewall.

     Or

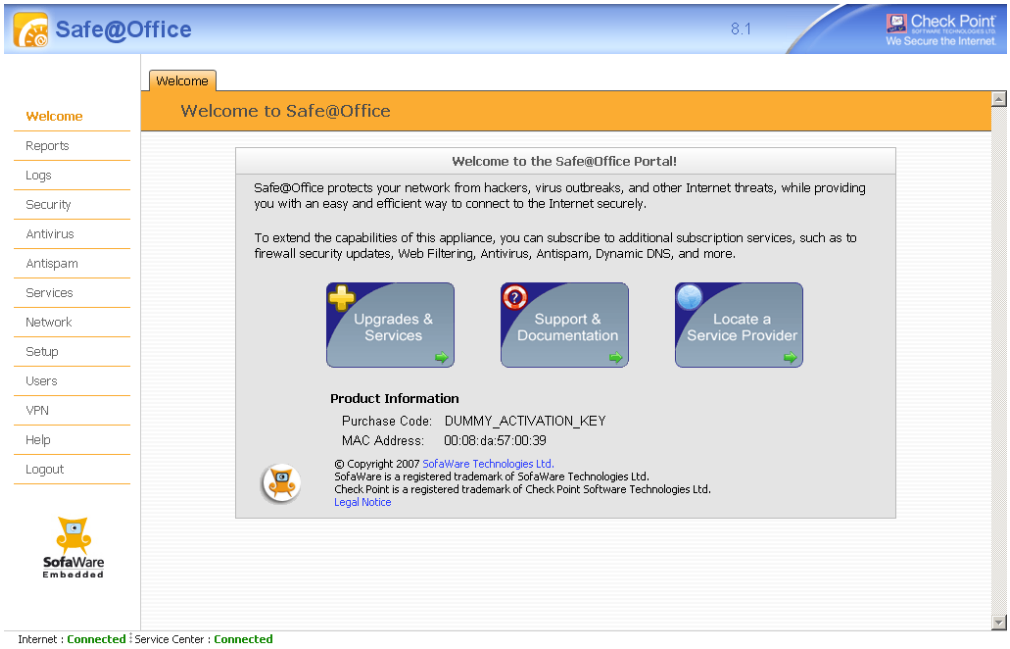
   - To log in through HTTPS (locally or remotely), follow the procedure ***Accessing the Safe@Office Portal Remotely*** on page 116.

The login page appears.



2. Type your username and password.
3. Click OK.

The Welcome page appears.


Safe@Office
8.1
Check Point
We Secure the Internet
Welcome
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare Embedded
Welcome to Safe@Office
Welcome to the Safe@Office Portal!
Safe@Office protects your network from hackers, virus outbreaks, and other Internet threats, while providing you with an easy and efficient way to connect to the Internet securely.
To extend the capabilities of this appliance, you can subscribe to additional subscription services, such as to firewall security updates, Web Filtering, Antivirus, Antispam, Dynamic DNS, and more.
Upgrades & Services
Support & Documentation
Locate a Service Provider
Product Information
Purchase Code: DUMMY_ACTIVATION_KEY
MAC Address: 00:08:da:57:00:39
© Copyright 2007 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice
Internet : Connected
Service Center : Connected

Accessing the Safe@Office Portal Remotely Using HTTPS

500 1000N

You can access the Safe@Office Portal remotely (from the Internet) through HTTPS. HTTPS is a protocol for accessing a secure Web server. It is used to transfer confidential user information. If desired, you can also use HTTPS to access the Safe@Office Portal from your internal network.

Note: In order to access the Safe@Office Portal remotely using HTTPS, you must first do both of the following:

- Configure your password, using HTTP. See ***Initial Login to the Safe@Office Portal*** on page 111.
- Configure HTTPS Remote Access. See ***Configuring HTTPS*** on page 728.

Note: Your browser must support 128-bit cipher strength. To check your browser's cipher strength, open Internet Explorer and click Help > About Internet Explorer.

To access the Safe@Office Portal from your internal network

- Browse to https://my.firewall.

  (Note that the URL starts with “https”, not “http”.)

  The Safe@Office Portal appears.

To access the Safe@Office Portal from the Internet

- Browse to https://<firewall_IP_address>:981.

  (Note that the URL starts with “https”, not “http”.)

  The following things happen in the order below:

  If this is your first attempt to access the Safe@Office Portal through HTTPS, the certificate in the Safe@Office appliance is not yet known to the browser, so the Security Alert dialog box appears.

  To avoid seeing this dialog box again, install the certificate of the destination Safe@Office appliance. If you are using Internet Explorer 6, do the following:

  a. Click View Certificate.

     The Certificate dialog box appears, with the General tab displayed.

  b. Click Install Certificate.

     The Certificate Import Wizard opens.

  c. Click Next.

  d. Click Next.

  e. Click Finish.

  f. Click Yes.

g. Click OK.
   The Security Alert dialog box reappears.
h. Click Yes.
   The Safe@Office Portal appears.

Using the Safe@Office Portal

The Safe@Office Portal is a Web-based management interface, which enables you to manage and configure the Safe@Office appliance operation and options.

The Safe@Office Portal consists of three major elements.

Table 26: Safe@Office Portal Elements

Element	Description
Main menu	Used for navigating between the various topics (such as Reports, Security, and Setup).
Main frame	Displays information and controls related to the selected topic. The main frame may also contain tabs that allow you to view different pages related to the selected topic.
Status bar	Shows your Internet connection and managed services status.

Main Frame
Main Menu
Status Bar
Safe@Office
8.1
Check Point
Welcome
Welcome to Safe@Office
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
Welcome to the Safe@Office Portal!
Safe@Office protects your network from hackers, virus outbreaks, and other Internet threats, while providing you with an easy and efficient way to connect to the Internet securely.
To extend the capabilities of this appliance, you can subscribe to additional subscription services, such as to firewall security updates, Web Filtering, Antivirus, Antispam, Dynamic DNS, and more.
Upgrades & Services
Support & Documentation
Locate a Service Provider
Product Information
Purchase Code: DUMMY_ACTIVATION_KEY
MAC Address: 00:08:da:57:00:39
© Copyright 2007 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice
SofaWare Embedded
Internet : Connected | Service Center : Connected

Figure 26: Safe@Office Portal

Main Menu

The main menu includes the following submenus.

Table 27: Main Menu Submenus

This submenu…	Does this…
Welcome	Displays general welcome information.
Reports	Provides reporting capabilities in terms of appliance status, traffic monitoring, active computers, established connections, and more.
Logs	Provides a general event log displaying appliance events, and a security event log displaying firewall events.
Security	Provides controls and options for setting the security of any computer in the network.
Antivirus	Allows you to configure VStream Antivirus settings.
Antispam	Allows you to configure VStream Antispam settings.
Services	Allows you to control your subscription to subscription services.
Network	Allows you to manage and configure your network settings and Internet connections.
Setup	Provides a set of tools for managing your Safe@Office appliance. Allows you to upgrade your license and firmware and to configure HTTPS access to your Safe@Office appliance.
Users	Allows you to manage Safe@Office appliance users.
VPN	Allows you to manage, configure, and log in to VPN sites.
Help	Provides context-sensitive online help.

This submenu…	Does this…
Logout	Allows you to log out of the Safe@Office Portal.

Main Frame

The main frame displays the relevant data and controls pertaining to the menu and tab you select. These elements sometimes differ depending on what model you are using. The differences are described throughout this guide.

Status Bar

The status bar is located at the bottom of each page. It displays the fields below, as well as the date and time.

Table 28: Status Bar Fields

This field…	Displays this…
Internet	Your Internet connection status. The connection status may be one of the following: • Connected. The Safe@Office appliance is connected to the Internet. • Connected – Probing OK. Connection probing is enabled and has detected that the Internet connectivity is OK. • Connected – Probing Failed. Connection probing is enabled and has detected problems with the Internet connectivity. • Not Connected. The Internet connection is down. • Establishing Connection. The Safe@Office appliance is connecting to the Internet. • Contacting Gateway. The Safe@Office appliance is trying to contact the Internet default gateway. • Disabled. The Internet connection has been manually disabled. Note: You can configure both a primary and a secondary Internet connection. When both connections are configured, the Status bar displays both statuses. For example “Internet [Primary]: Connected”. For information on configuring a secondary Internet connection, see ***Configuring the Internet Connection*** on

This field...	Displays this...
	page 125.
Service Center	Displays your subscription services status. Your Service Center may offer various subscription services. These include the firewall service and optional services such as Web Filtering and Email Antivirus. Your subscription services status may be one of the following: • Not Subscribed. You are not subscribed to security services. • Connection Failed. The Safe@Office appliance failed to connect to the Service Center. • Connecting. The Safe@Office appliance is connecting to the Service Center. • Connected. You are connected to the Service Center, and security services are active.

Logging Out

500 1000N

Logging out terminates your administration session. Any subsequent attempt to connect to the Safe@Office Portal will require re-entering of the administration password.

To log out of the Safe@Office Portal

- Click Logout in the main menu.

  The Login page appears.

Chapter 5

Configuring the Internet Connection

This chapter describes how to configure and work with a Safe@Office Internet connection.

This chapter includes the following topics:

Overview 125
Using the Internet Wizard 126
Using Internet Setup 141
Setting Up Modems 176
Viewing Internet Connection Information 188
Enabling/Disabling the Internet Connection 190
Using Quick Internet Connection/Disconnection 190
Configuring a Backup Internet Connection 191
Configuring WAN Load Balancing 192

Overview

In order to access the Internet through your Safe@Office appliance, you must configure one of the following connection types:

- Ethernet-based connection

  You can configure an Ethernet-based connection in all models. An Ethernet-based connection can be connected to another network by means of a switch, a router, a bridge, or an Ethernet-enabled broadband modem.

  In ADSL models, the Ethernet-based connection is configured on the DMZ/WAN2 port. In non-ADSL models, you can use the WAN port, the DMZ/WAN2 port, or both ports for an Ethernet-based Internet connection.

- Direct ADSL connection

  You can configure a direct ADSL connection in Safe@Office ADSL models only. These models include an integrated ADSL modem, which enables you to connect the appliance directly to your ADSL line without using an additional modem or router.

You can configure your Internet connection using any of the following setup tools:

- Setup Wizard. Guides you through the Safe@Office appliance setup step by step. The first part of the Setup Wizard is the Internet Wizard. For further information on the Setup Wizard, see ***Setting Up the Safe@Office Appliance*** on page 107.
- Internet Wizard. Guides you through the Internet connection configuration process step by step. For further information, see ***Using the Internet Wizard*** on page 126.
- Internet Setup. Offers the following advanced setup options:
  - Configure two Internet connections.
    For information, see ***Configuring a Backup Internet Connection*** on page 191.
  - Enable Traffic Shaper for traffic flowing through the connection.
    For information on Traffic Shaper, see ***Using Traffic Shaper*** on page 293.
  - Configure a dialup Internet connection.
    Before configuring the connection, you must first set up the modem. For information, see ***Setting Up Modems*** on page 176.

Using the Internet Wizard

500 1000N

The Internet Wizard allows you to configure your Safe@Office appliance for Internet connection quickly and easily through its user-friendly interface.

Note: The first time you log in to the Safe@Office Portal, the Internet Wizard starts automatically as part of the Setup Wizard. In this case, you should skip to step 3 in the following procedure.

Configuring an Ethernet-Based Connection on Non-ADSL Models

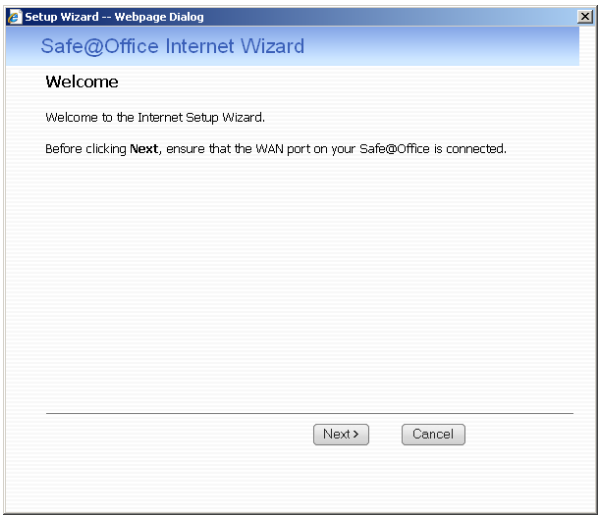
To configure an Ethernet-Based connection

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

2. Click Internet Wizard.

   The Internet Wizard opens with the Welcome page displayed.


Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Welcome
Welcome to the Internet Setup Wizard.
Before clicking Next, ensure that the WAN port on your Safe@Office is connected.
Next >
Cancel

3. Click Next.

The Internet Connection Method dialog box appears.

Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Internet Connection Method
Select your Internet connection method:
PPPoE (PPP over Ethernet)
PPTP
Cable Modem
Static IP
DHCP (Dynamic IP)
If you are not sure how to proceed, please contact your Internet Service Provider (ISP).
< Back
Next >
Cancel

4. Select the Internet connection method you want to use for connecting to the Internet.

   If you are uncertain regarding which connection method to use, contact your ISP.

Note: If you selected PPTP or PPPoE, do not use your dial-up software to connect to the Internet.

5. Click Next.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 129.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 131.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 132.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 133.

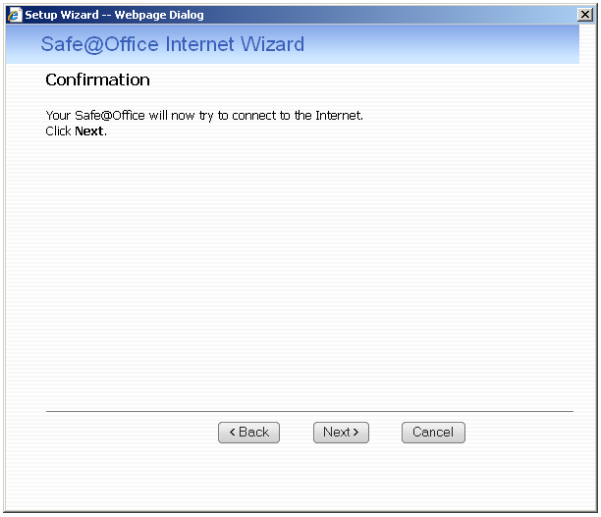
   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 134.

Using a PPPoE Connection

If you selected the PPPoE (PPP over Ethernet) connection method, the PPP Configuration dialog box appears.

1. Complete the fields using the information in the following table.
2. Click Next.

   The Confirmation screen appears.

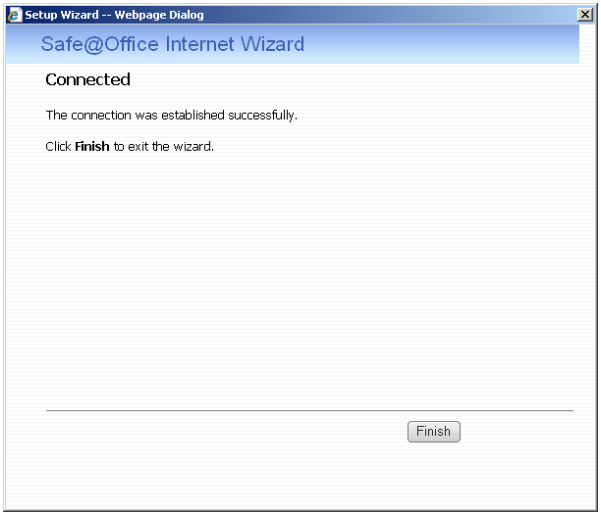


3. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.



4. Click Finish.

Table 29: PPPoE Connection Fields

In this field...	Do this...
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.
Service	Type your service name. This field can be left blank.

Using a PPTP Connection

If you selected the PPTP connection method, the PPP Configuration dialog box appears.

1. Complete the fields using the information in the following table.
2. Click Next.

   The Confirmation screen appears.
3. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.
4. Click Finish.

Table 30: PPTP Connection Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.
Service	Type your service name.
Server IP	Type the IP address of the PPTP modem.
Internal IP	Type the local IP address required for accessing the PPTP modem.
Subnet Mask	Select the subnet mask of the PPTP modem.

Using a Cable Modem Connection

No further settings are required for a cable modem connection. The Confirmation screen appears.

1. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.

2. Click Finish.

Using a Static IP Connection

If you selected the Static IP connection method, the Static IP Configuration dialog box appears.

1. Complete the fields using the information in the following table.
2. Click Next.

   The Confirmation screen appears.
3. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.
4. Click Finish.

Table 31: PPPoE Connection Fields

In this field…	Do this…
IP Address	Type the static IP address of your Safe@Office appliance.
Subnet Mask	Select the subnet mask that applies to the static IP address of your Safe@Office appliance.
Default Gateway	Type the IP address of your ISP's default gateway.
Primary DNS Server	Type the IP address of your ISP's primary DNS server.
Secondary DNS Server	Type the IP address of your ISP's secondary DNS server. This field is optional.
WINS Server	Type the IP address of your ISP's WINS server. This field is optional.

Using a DHCP Connection

No further settings are required for a DHCP (Dynamic IP) connection. The Confirmation screen appears.

1. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.

2. Click Finish.

Configuring an Ethernet-Based Connection on ADSL Models

ADSL

Note: In ADSL models, an Ethernet-based connection is made on the DMZ/WAN2 port.

To configure an Ethernet-based connection

1. Click Network in the main menu, and click the Internet tab.

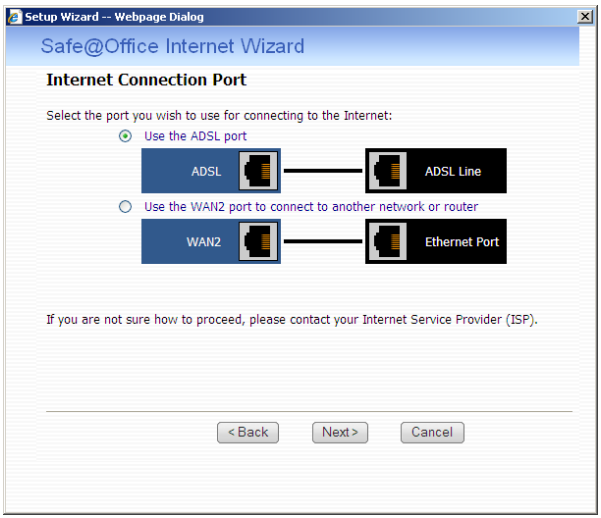
   The Internet page appears.

2. Click Internet Wizard.

   The Internet Wizard opens with the Welcome page displayed.

3. Click Next.

   The Internet Connection Port dialog box appears.


Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Internet Connection Port
Select the port you wish to use for connecting to the Internet:
Use the ADSL port
ADSL
ADSL Line
Use the WAN2 port to connect to another network or router
WAN2
Ethernet Port
If you are not sure how to proceed, please contact your Internet Service Provider (ISP).
< Back
Next >
Cancel

4. Click Use the WAN2 port to connect to another network or router.
5. Click Next.

The Internet Connection Method dialog box appears.

Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Internet Connection Method
Select your Internet connection method:
PPPoE (PPP over Ethernet)
PPTP
Cable Modem
Static IP
DHCP (Dynamic IP)
If you are not sure how to proceed, please contact your Internet Service Provider (ISP).
< Back
Next >
Cancel

6. Select the Internet connection method you want to use for connecting to the Internet.
7. Click Next.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 129.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 131.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 132.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 133.

   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 134.

Configuring a Direct ADSL Connection

ADSL

To configure a direct ADSL connection

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

2. Click Internet Wizard.

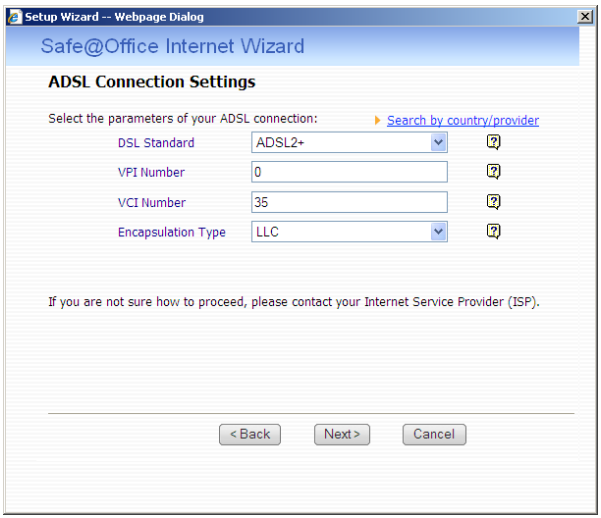
   The Internet Wizard opens with the Welcome page displayed.

3. Click Next.

   The Internet Connection Port dialog box appears.

4. Click Use the ADSL port.

   The ADSL Connection Settings dialog box appears.

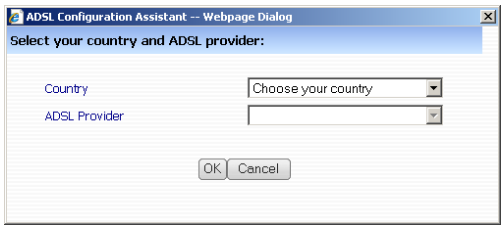


5. Do one of the following:

   - To automatically fill in the supported ADSL settings for your ISP, do the following:

     1) Click Search by country and ISP.

The ADSL Configuration Assistant opens.



2) In the Country drop-down list, select your country.

3) In the ISP / Telco drop-down list, select your ISP or telephone company.

   The ADSL Configuration Assistant closes, and the fields are filled in with the correct values for your ISP.

- To manually fill in the supported ADSL settings for your ISP, complete the fields using the information in the following table.

6. Click Next.

   The Internet Connection Method dialog box appears.

Setup Wizard -- Webpage Dialog
Safe@Office Internet Wizard
Internet Connection Method
Select your Internet connection method:
PPPoE (PPP over Ethernet)
PPPoA (PPP over ATM)
Static IP
DHCP (Dynamic IP)
If you are not sure how to proceed, please contact your Internet Service Provider (ISP).
< Back
Next >
Cancel

7. Select the Internet connection method you want to use for connecting to the Internet.

8. Click Next.

If you chose PPPoE or PPPoA, continue at ***Using a PPPoE or PPPoA Connection*** on page 140.

If you chose Static IP, continue at ***Using a Static IP Connection*** on page 133.

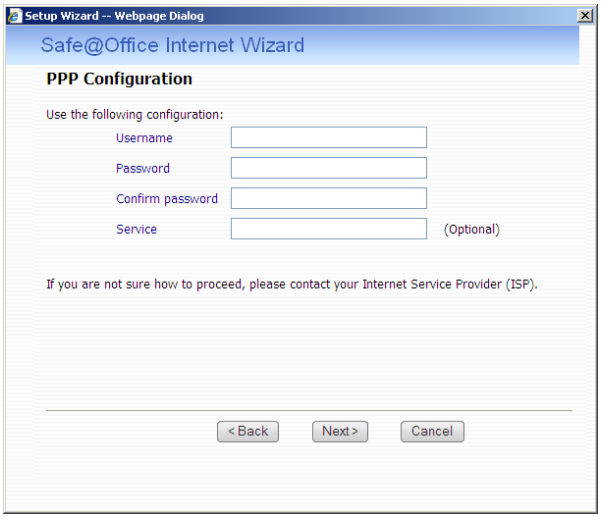
If you chose DHCP, continue at ***Using a DHCP Connection*** on page 134.

Table 32: ADSL Connection Fields

In this field…	Do this…
DSL Standard	Select the standard to support for the DSL line, as specified by your ISP. This can be one of the following: • ADSL2 • ADSL2+ • Multimode • T.1413 • G.lite • G.DMT
VPI Number	Type the VPI number to use for the ATM virtual path, as specified by your ISP.
VCI Number	Type the VCI number to use for the ATM virtual circuit, as specified by your ISP.
Encapsulation Type	Select the encapsulation type to use for the DSL line, as specified by your ISP. This can be one of the following: • LLC • VCMUX

Using a PPPoE or PPPoA Connection

If you selected the PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM) connection method, the PPP Configuration dialog box appears.



1. Complete the fields using the information in the following table.
2. Click Next.

   The Confirmation screen appears.
3. Click Next.

   The system attempts to connect to the Internet via the specified connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.
4. Click Finish.

Table 33: PPPoE Connection Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.

Using Internet Setup

500 1000N

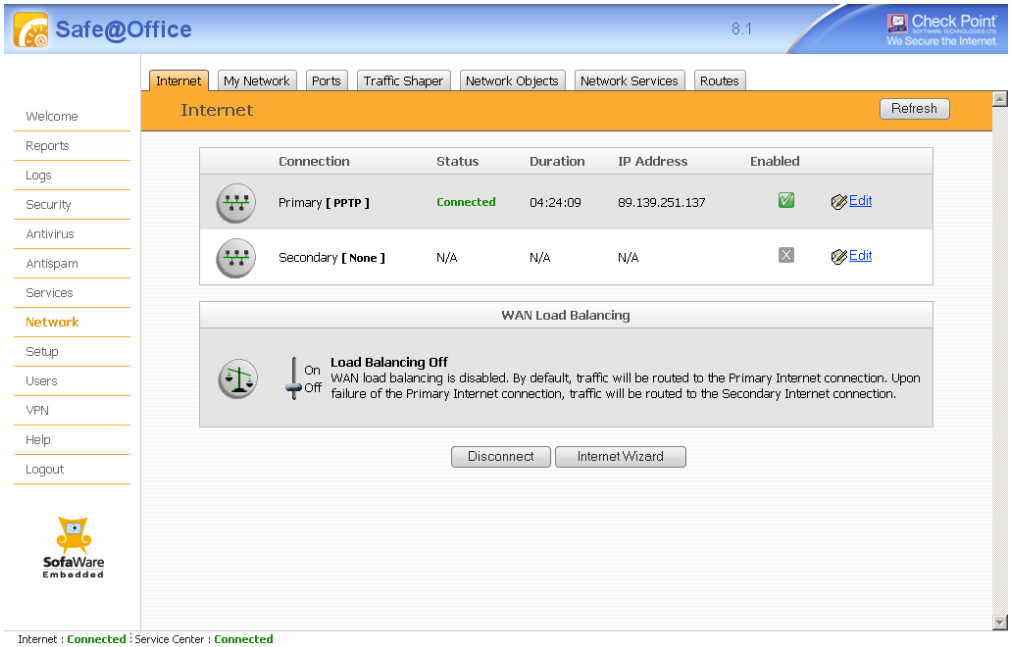
Internet Setup allows you to manually configure your Internet connection.

For information on configuring bridged Internet connections, see ***Adding Internet Connections to Bridges*** on page 274.

To configure the Internet connection using Internet Setup

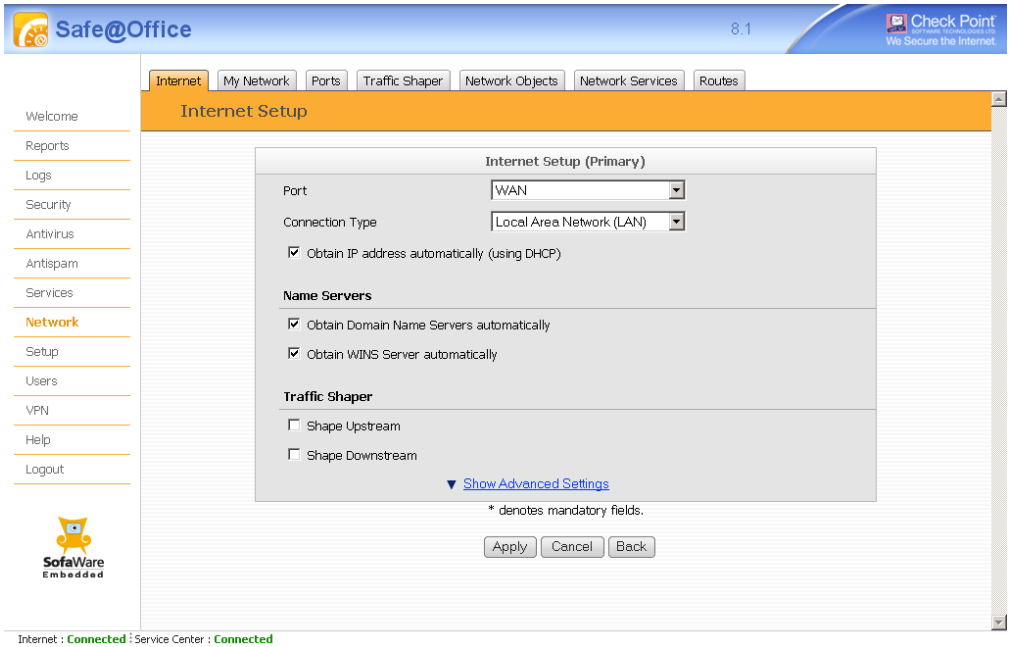
1. Click Network in the main menu, and click the Internet tab.

The **Internet** page appears.



2. Next to the desired Internet connection, click **Edit**.

The Internet Setup page appears.



3. Do one of the following:

   - To configure an ADSL connection using the internal ADSL modem, continue at ***Configuring a Direct ADSL Connection*** on page 144.

     This option is available in ADSL models only.
   - To configure an Ethernet-based connection, continue at ***Configuring an Ethernet-Based Connection*** on page 153.
   - To configure a Dialup connection, continue at ***Configuring a Dialup Connection*** on page 166.
   - To configure no connection, continue at ***Using No Connection*** on page 168.

Configuring a Direct ADSL Connection

1. In the Port drop-down list, select ADSL.
2. Do one of the following:
   - To automatically fill in the supported ADSL settings for your ISP, do the following:
     1) Click Search by country and ISP.

        The ADSL Configuration Assistant opens.
     2) In the Country drop-down list, select your country.
     3) In the ISP / Telco drop-down list, select your ISP or telephone company.

        The ADSL Configuration Assistant closes. The Connection Type drop-down list and the ADSL Link Settings fields are filled in with the correct values for your ISP.
   - To manually fill in the supported ADSL settings for your ISP, in the Connection Type drop-down list, select the Internet connection type you intend to use.

   The display changes according to the selected connection type.

   For PPPoA, continue at ***Using a PPPoA Connection*** on page 145.

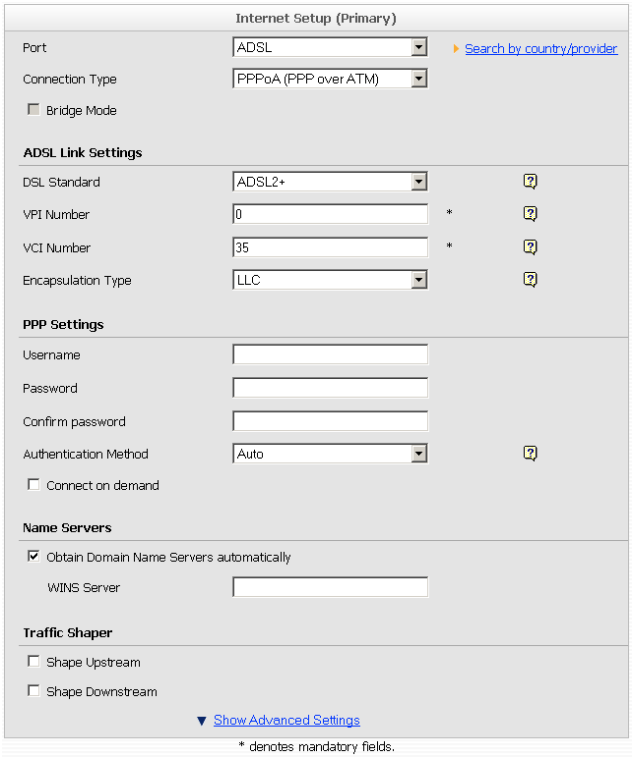
   For EoA, continue at ***Using an EoA Connection*** on page 147.

   For PPPoE, continue at ***Using a PPPoE Connection*** on page 149.

   For IPoA, continue at ***Using an IPoA (IP over ATM) Connection*** on page 151.

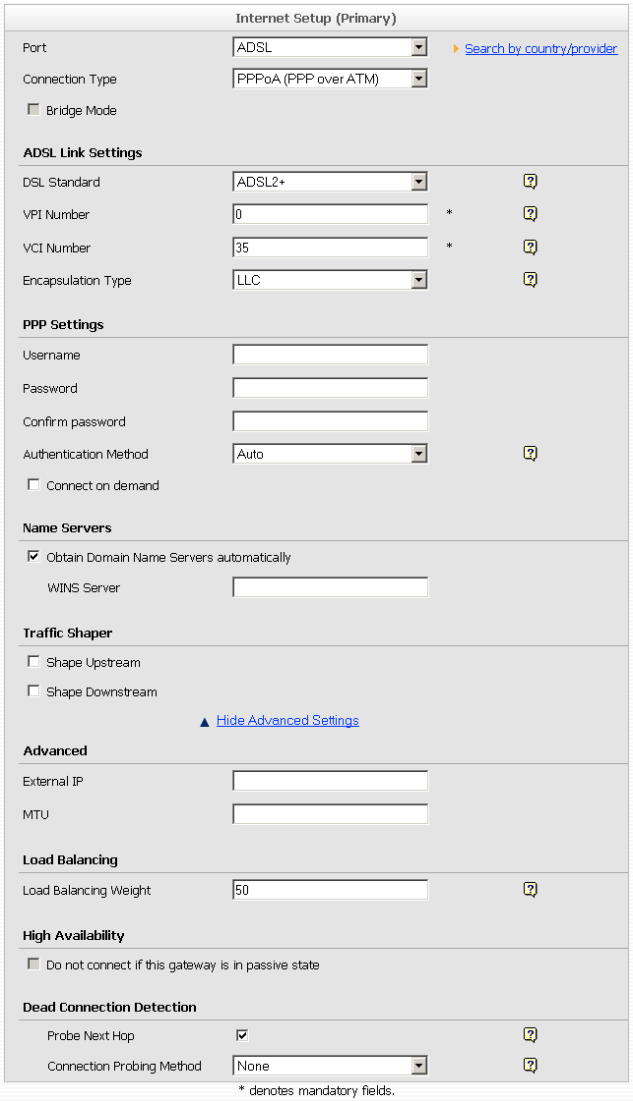
   For information on configuring bridged connections, see ***Adding Internet Connections to Bridges*** on page 274.

Using a PPPoA (PPP over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

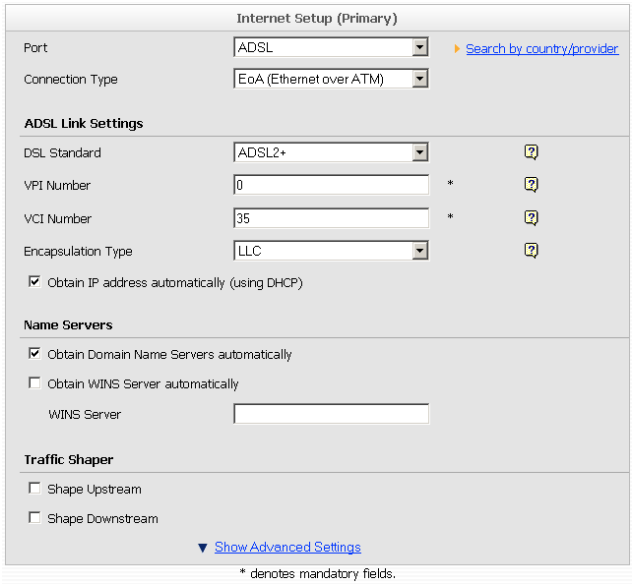


2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

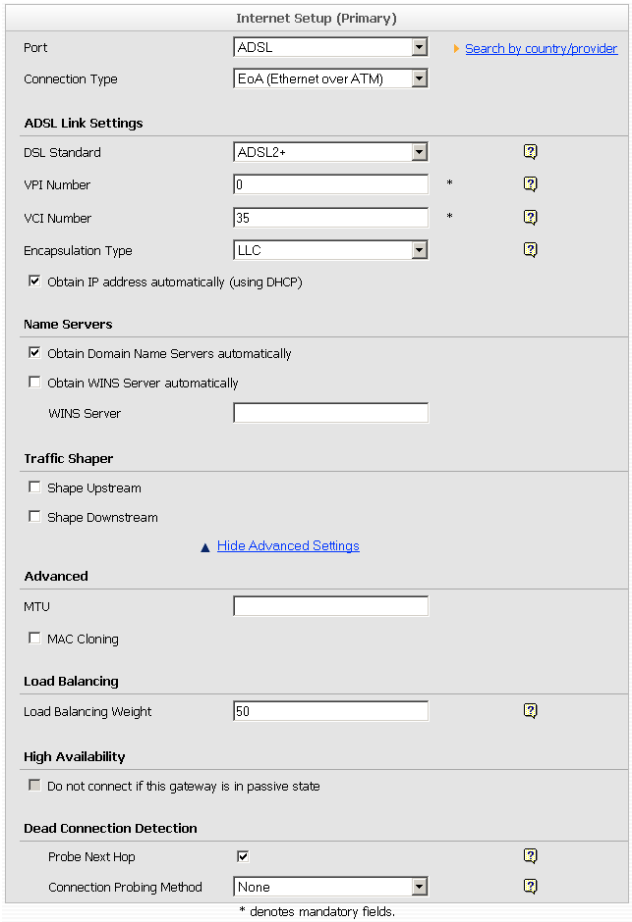
Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using an EoA (Ethernet over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

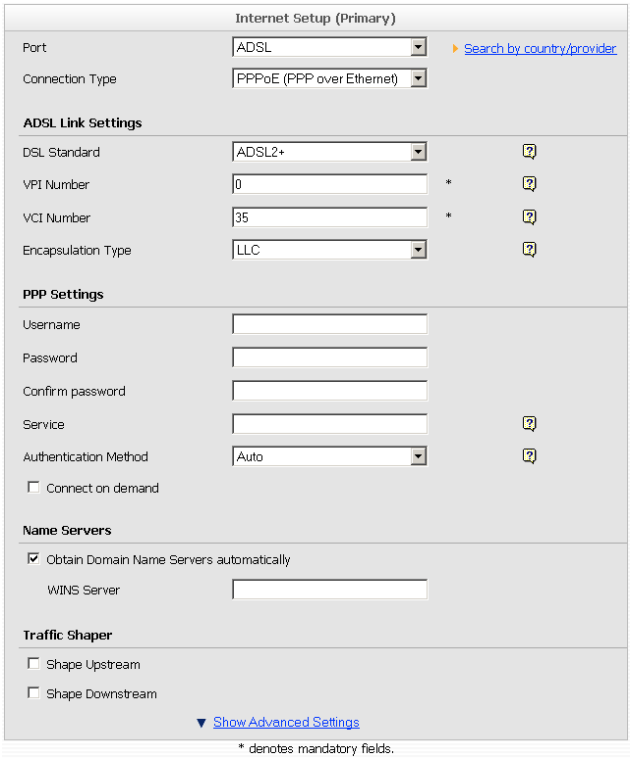


2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

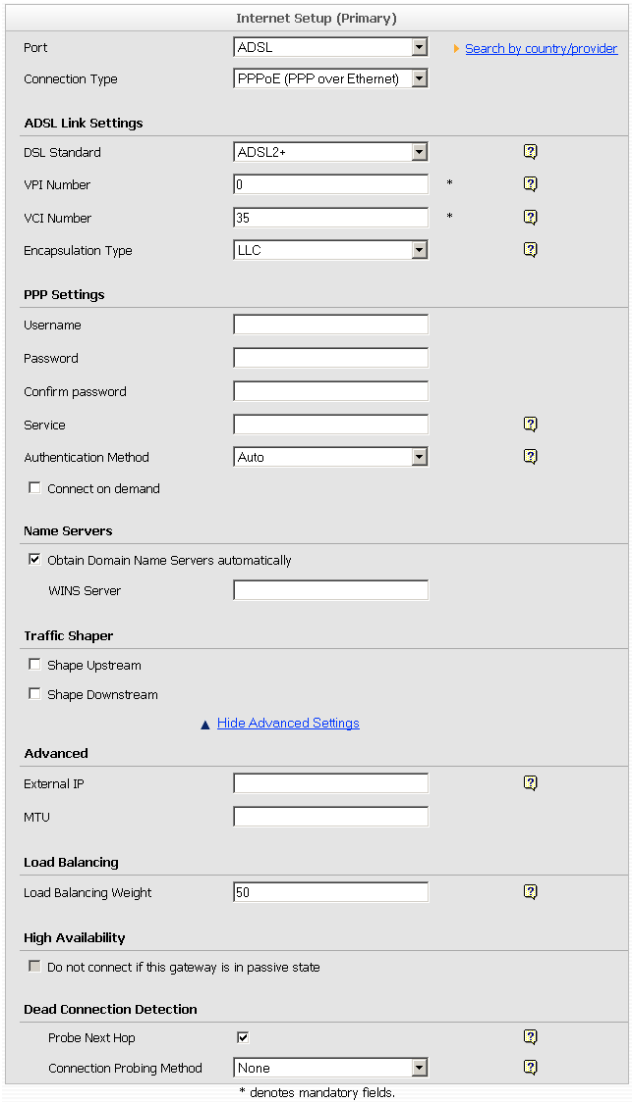
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE (PPP over Ethernet) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

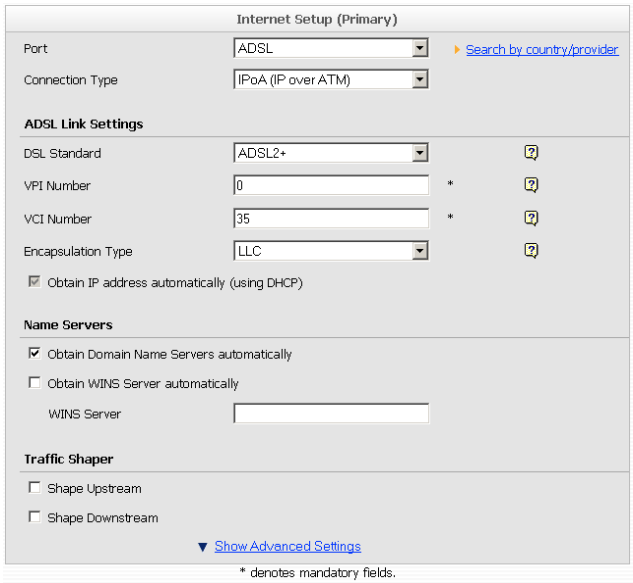


2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

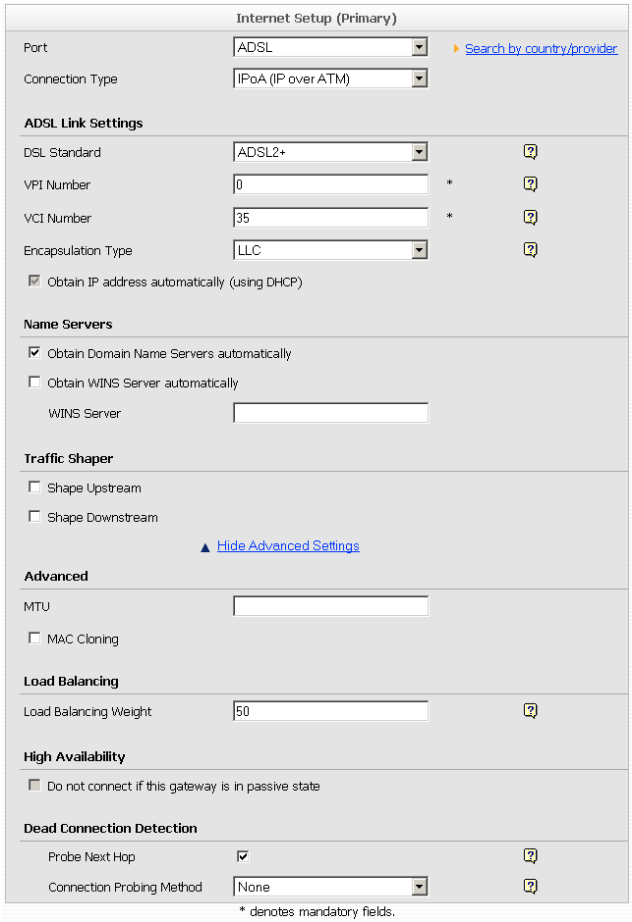
Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using an IPoA (IP over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.



2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Configuring an Ethernet-Based Connection

500 1000N

1. In the Port drop-down list, do one of the following:
   - To configure an Ethernet-based connection through the WAN port, select WAN.
   - To configure an Ethernet-based connection through the DMZ/WAN2 port, select WAN2.

     This option is available in non-ADSL models only.
   - To configure an Ethernet-based connection through a LAN port, select the desired LAN port.

     This option is available with the Power Pack license only.

   The selected port is automatically configured for use with an Internet connection. For information on viewing a port's status, see ***Viewing Port Statuses.*** on page 247
2. In the Connection Type drop-down list, select the Internet connection type you intend to use.

   The display changes according to the connection type you selected.

   If you chose LAN, continue at ***Using a LAN Connection*** on page 154.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 156.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 158.

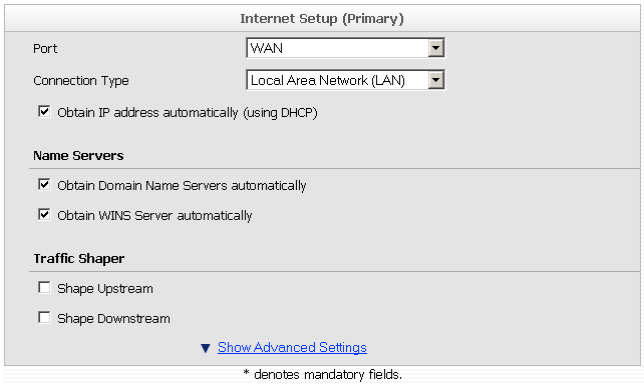
   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 160.

   If you chose L2TP, continue at ***Using an L2TP Connection*** on page 162.

   If you chose Telstra, continue at ***Using a Telstra (BPA) Connection*** on page 164.

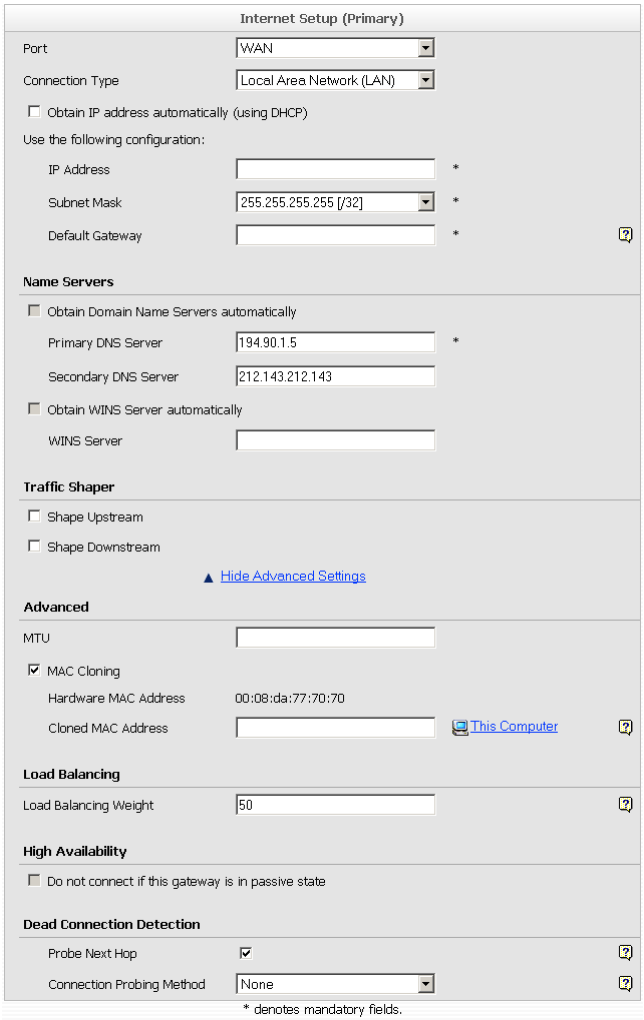
   For information on configuring bridged connections, see ***Adding Internet Connections to Bridges*** on page 274.

Using a LAN Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

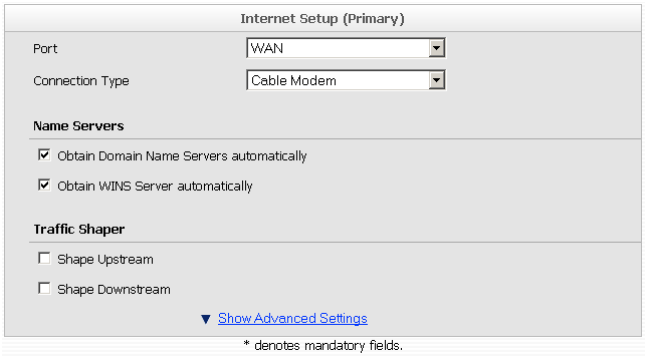


2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

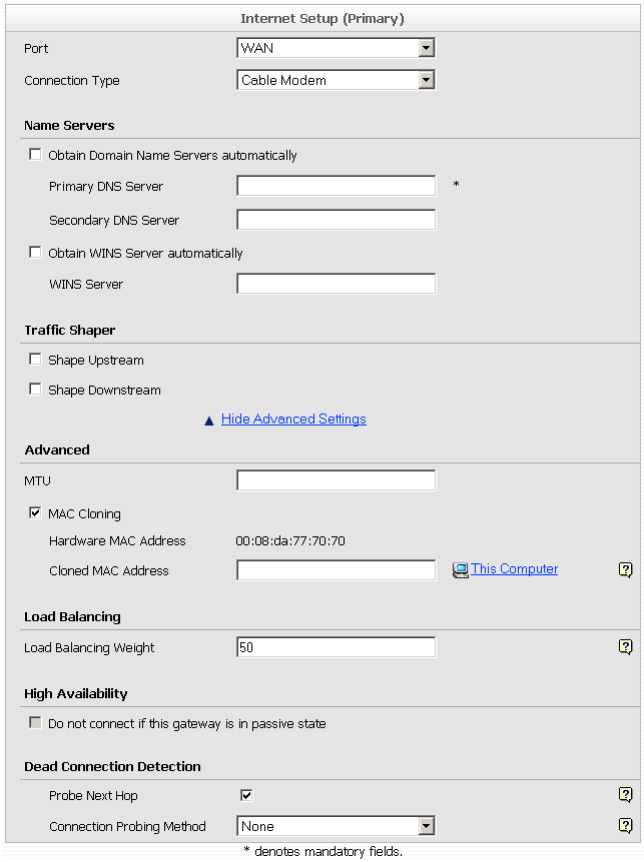
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.



2. Click Apply.

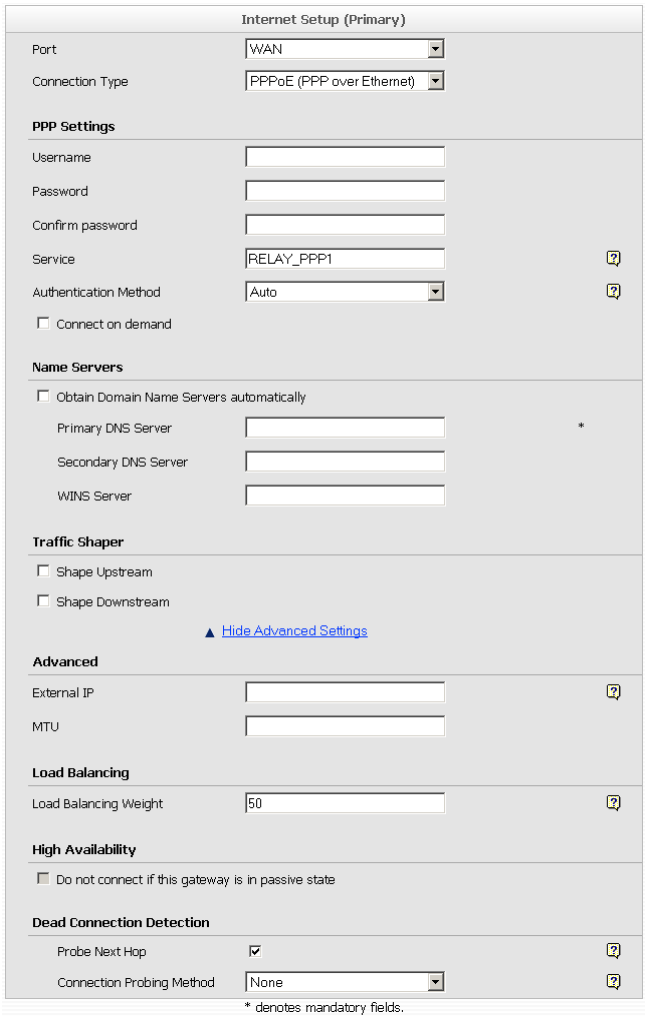
   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

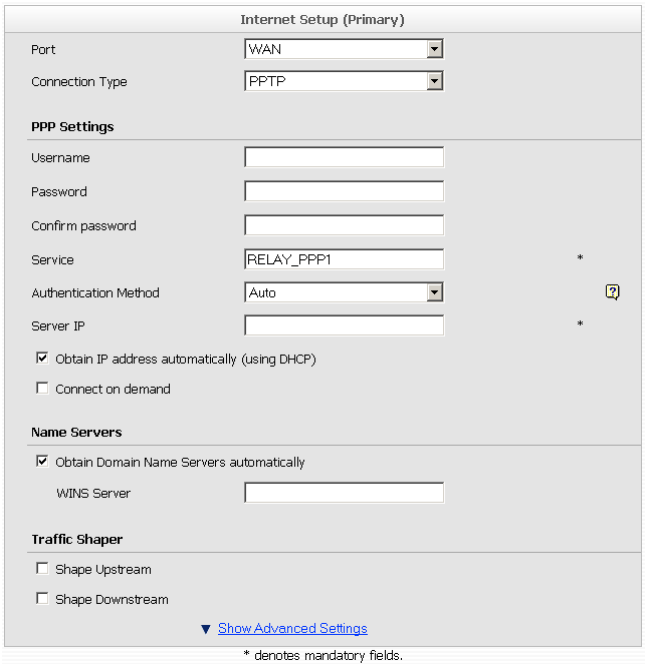


2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

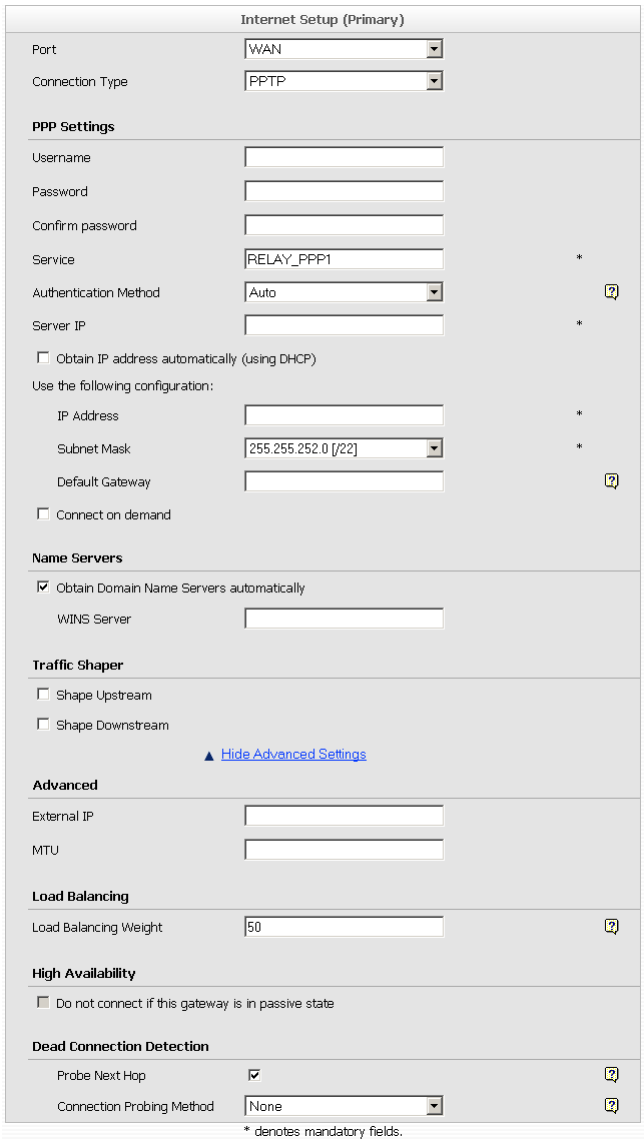
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPTP Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.

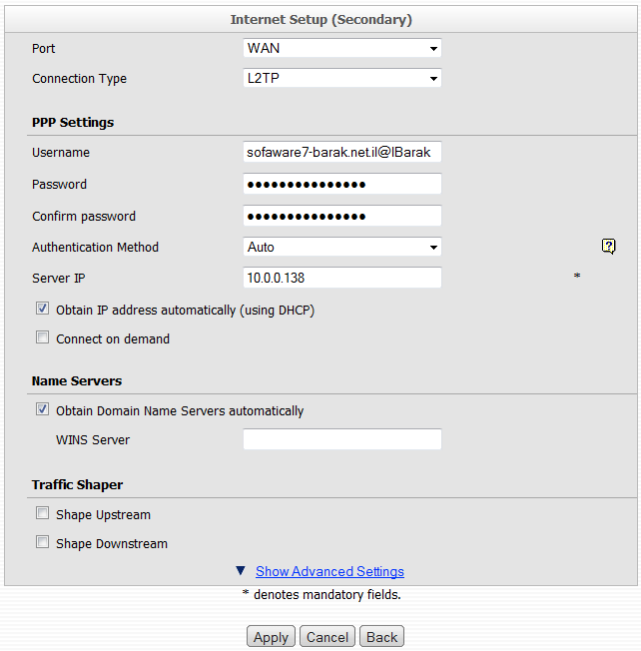


2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

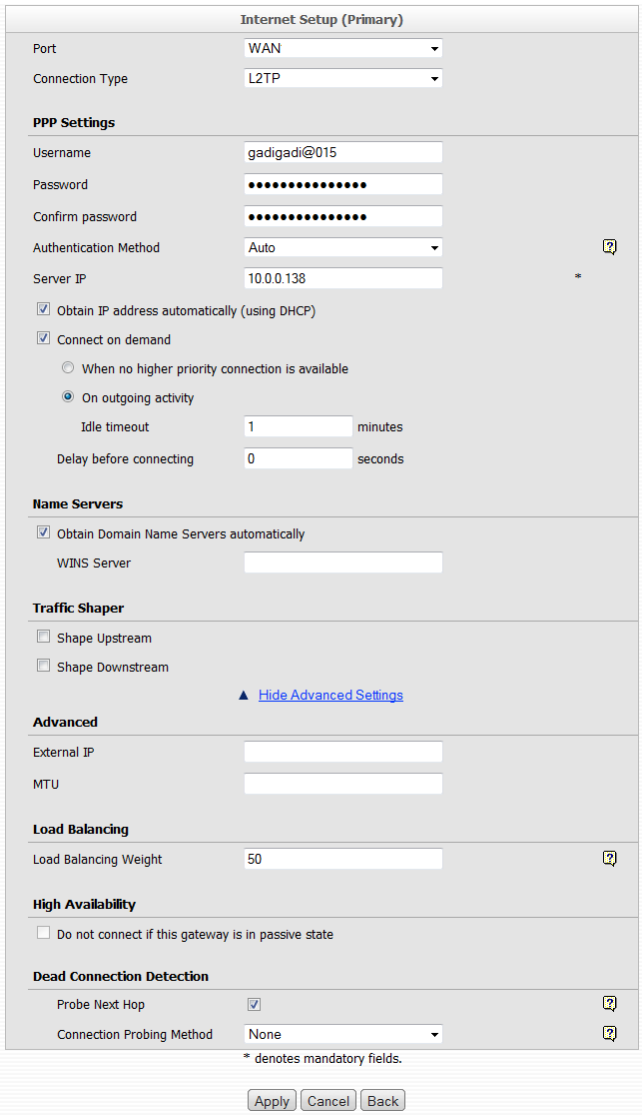
Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using an L2TP Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.



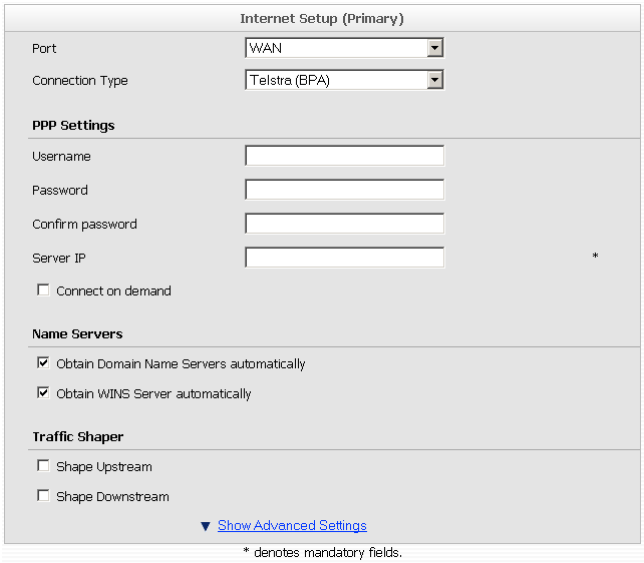
2. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status “Connected”.

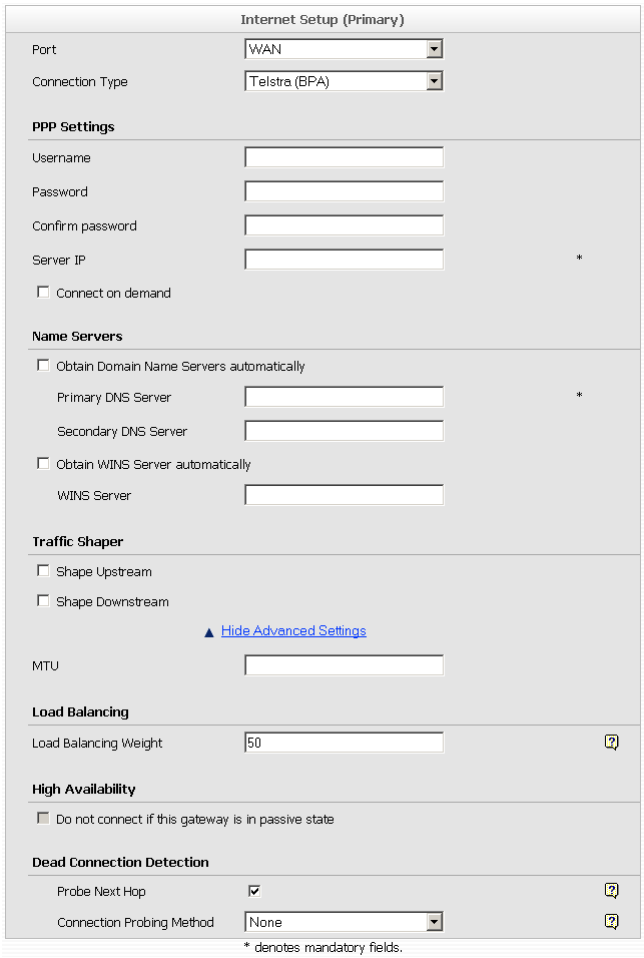
Using a Telstra (BPA) Connection

Use this Internet connection type only if you are subscribed to Telstra® BigPond™ Internet. Telstra BigPond is a trademark of Telstra Corporation Limited.



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.



2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Configuring a Dialup Connection

500 1000N

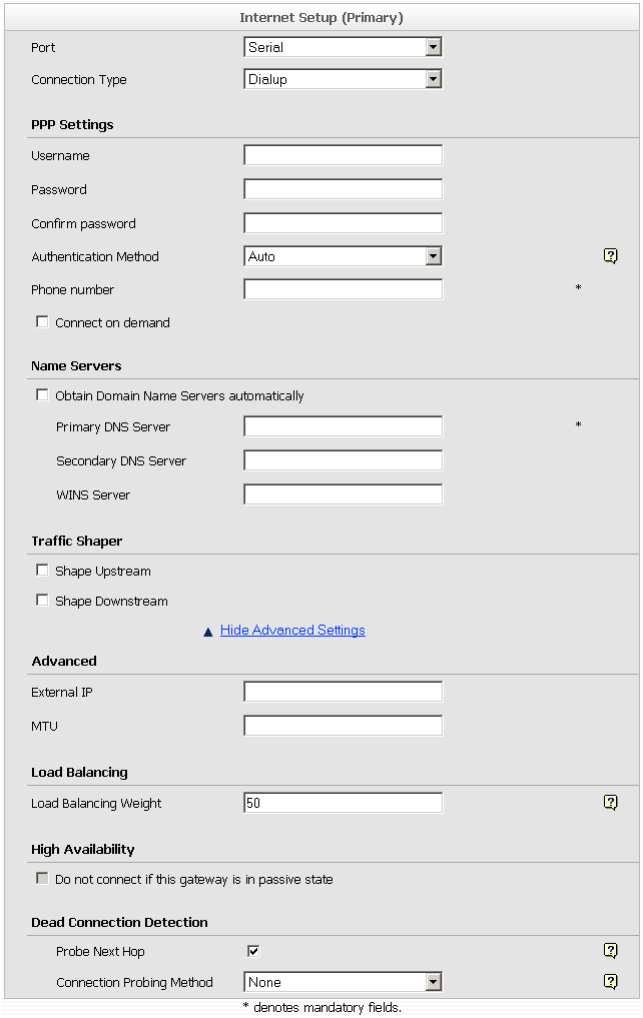
Note: To use this connection type, you must first set up the dialup or cellular modem. For information, see ***Setting Up Modems*** on page *176*.

1. In the Port drop-down list, do one of the following:
   - To configure a Dialup connection on the Serial port (using a connected RS232 modem), select Serial.
   - To configure a Dialup connection on a USB port (using a connected USB modem), select Cellular Modem.

   The Connection Type field displays Dialup.

2. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 168.

New fields appear, depending on the check boxes you selected.



3. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Establishing Connection”. This may take several seconds.

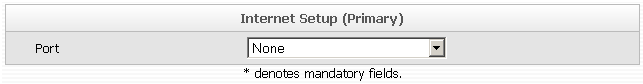
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Configuring No Connection

500 1000N

1. In the Port drop-down list, select None.

   The fields disappear.



2. Click Apply.

Table 34: Internet Setup Fields

In this field…	Do this…
ADSL Link Settings	
DSL Standard	Select the standard to support for the DSL line, as specified by your ISP.
VPI Number	Type the VPI number to use for the ATM virtual path, as specified by your ISP.
VCI Number	Type the VCI number to use for the ATM virtual circuit, as specified by your ISP.
Encapsulation Type	Select the encapsulation type to use for the DSL line, as specified by your ISP.
PPP Settings	
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.

In this field...	Do this...
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
Authentication Method	Specify the authentication method to use for PPP connections, by selecting one of the following: • Auto. If possible, use CHAP; otherwise, use PAP. This is the default. • PAP • CHAP
Server IP	If you selected PPTP, type the IP address of the PPTP server as given by your ISP. If you selected Telstra (BPA), type the IP address of the Telstra authentication server as given by Telstra.
Phone Number	If you selected Dialup, type the phone number that the modem should dial, as given by your ISP.
Connect on demand	Select this option if you do not want the appliance to be constantly connected to the Internet. The appliance will establish a connection only under certain conditions. This option is useful when configuring a backup connection. For information, see ***Configuring a Backup Internet Connection*** on page 191.

In this field…	Do this…
When no higher priority connection is available	Select this option to specify that the appliance should only establish a connection in the following cases: • When no other connection exists, and the Safe@Office appliance is not acting as a Backup appliance. If another connection opens, the appliance will disconnect. For information on configuring the appliance as a Backup or Master, see ***Configuring High Availability*** on page 281. • When there is interesting traffic (that is, traffic for which no static route is defined).
On outgoing activity	Select this option to specify that the appliance should only establish a connection if no other connection exists, and there is outgoing activity (that is, packets need to be transmitted to the Internet). If another connection opens, or if the connection times out, the appliance will disconnect.
Idle timeout	Type the amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the appliance will disconnect. The default value is 1.
Delay before connecting	Type the amount of time (in seconds) that the appliance should wait to re-connect to the Internet, if the connection goes down. If you have an unstable Internet connection that tends to go down and then return almost immediately, this setting allows you to avoid unnecessary and costly dialing during outage periods, by deferring re-connection for a few seconds. The default value is 0.
Obtain IP address automatically (using DHCP)	Clear this option if you do not want the Safe@Office appliance to obtain an IP address automatically using DHCP.

In this field...	Do this...
IP Address	Type the static IP address of your Safe@Office appliance.
Subnet Mask	Select the subnet mask that applies to the static IP address of your Safe@Office appliance.
Default Gateway	Type the IP address of your ISP's default gateway.
Name Servers	
Obtain Domain Name Servers automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure DNS servers.
Obtain WINS Server automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure the WINS server.
Primary DNS Server	Type the IP address of your ISP's primary DNS server.
Secondary DNS Server	Type the IP address of your ISP's secondary DNS server.
WINS Server	Type the IP address of your ISP's WINS server.
Traffic Shaper	
Shape Upstream: Link Rate	Select this option to enable Traffic Shaper for outgoing traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured upstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on

In this field...	Do this...
	page 293.
Shape Downstream: Link Rate	Select this option to enable Traffic Shaper for incoming traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured downstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on page 293.
Advanced	
External IP	If you selected PPTP, type the IP address of the PPTP client as given by your ISP. If you selected PPPoE, this field is optional, and you do not have to fill it in unless your ISP has instructed you to do so.
MTU	This field allows you to control the maximum transmission unit size. As a general recommendation you should leave this field empty. If however you wish to modify the default MTU, it is recommended that you consult with your ISP first and use MTU values between 1300 and 1500.
MAC Cloning	A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, you must select this option to clone a MAC address.

In this field...	Do this...
	Note: When configuring MAC cloning for the secondary Internet connection, the DMZ/WAN2 port must be configured as WAN2; otherwise this field is disabled. For information on configuring ports, see ***Managing Ports*** on page 246.
Hardware MAC Address	This field displays the Safe@Office appliance's MAC address. This field is read-only.
Cloned MAC Address	Do one of the following: • Click This Computer to automatically "clone" the MAC address of your computer to the Safe@Office appliance. • If the ISP requires authentication using the MAC address of a different computer, type the MAC address in this field. Note: In the secondary Internet connection, this field is enabled only if the DMZ/WAN2 port is set to WAN2.
Load Balancing	
Load Balancing Weight	If you are using WAN load balancing, type a value indicating the amount of traffic that should be routed though this connection relative to the other connection. For example, if you assign the primary connection a weight of 100, and you assign the secondary connection a weight of 50, twice as much traffic will be routed through the primary connection as through the secondary connection. To ensure full utilization of both Internet connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths. The default value is 50. For information on WAN load balancing, see ***Configuring WAN Load***

In this field...	Do this...
	Balancing on page 192.
High Availability	The High Availability area only appears in Safe@Office <500PP>.
Do not connect if this gateway is in passive state	If you are using High Availability (HA), select this option to specify that the gateway should connect to the Internet only if it is the Active Gateway in the HA cluster. This is called WAN HA. This field is only enabled if HA is configured. For information on HA, see ***Configuring High Availability*** on page 281.
Dead Connection Detection	
Probe Next Hop	Select this option to automatically detect loss of connectivity to the default gateway. If you selected LAN, this is done by sending ARP requests to the default gateway. If you selected PPTP, PPPoE, or Dialup, this is done by sending PPP echo reply (LCP) messages to the PPP peer. By default, if the default gateway does not respond, the Internet connection is considered to be down. If it is determined that the Internet connection is down, and two Internet connections are defined, a failover will be performed to the second Internet connection, ensuring continuous Internet connectivity. This option is selected by default.

In this field...	Do this...
Connection Probing Method	While the Probe Next Hop option checks the availability of the next hop router, which is usually at your ISP, connectivity to the next hop router does not always indicate that the Internet is accessible. For example, if there is a problem with a different router at the ISP, the next hop will be reachable, but the Internet might be inaccessible. Connection probing is a way to detect Internet failures that are more than one hop away. Specify what method to use for probing the connection, by selecting one of the following: • None. Do not perform Internet connection probing. Next hop probing will still be used, if the Probe Next Hop check box is selected. This is the default value. • Ping Addresses. Ping anywhere from one to three servers specified by IP address or DNS name in the 1, 2, and 3 fields. If for 45 seconds none of the defined servers respond to pinging, the Internet connection is considered to be down. Use this method if you have reliable servers that can be pinged, that are a good indicator of Internet connectivity, and that are not likely to fail simultaneously (that is, they are not at the same location). • Probe DNS Servers. Probe the primary and secondary DNS servers. If for 45 seconds neither gateway responds, the Internet connection is considered to be down. Use this method if the availability of your DNS servers is a good indicator for the availability of Internet connectivity. • Probe VPN Gateway (RDP). Send RDP echo requests to up to three Check Point VPN gateways specified by IP address or DNS name in the 1, 2, and 3 fields. If for 45 seconds none of the defined gateways respond, the Internet connection is considered to be down. Use this option if you have Check Point VPN gateways, and you want loss of connectivity to these gateways to trigger ISP failover to an Internet connection from which these gateways are reachable.

In this field...	Do this...
1, 2, 3	If you chose the Ping Addresses connection probing method, type the IP addresses or DNS names of the desired servers. If you chose the Probe VPN Gateway (RDP) connection probing method, type the IP addresses or DNS names of the desired VPN gateways. You can clear a field by clicking Clear.

Setting Up Modems

500 1000N

You can use a connected modem as a primary or secondary Internet connection method. This is useful in locations where broadband Internet access is unavailable.

When used as a backup Internet connection, the modem can be automatically disconnected when not in use. For information on setting up a backup connection, see ***Configuring a Backup Internet Connection*** on page 191.

The Safe@Office appliance supports the connecting following modems:

- RS232 dialup modem (regular or ISDN)

  You can connect one RS232 to the appliance's Serial port.

  See ***Setting Up an RS232 Modem*** on page 177.

- USB-based modems, including dialup (PSTN/ISDN) and cellular (GPRS/EVDO/3G) modems

  You can connect up to two USB-based modems to the appliance's USB port.

  See ***Setting Up a USB Modem*** on page 181.

Note: Only one USB modem can be used at a time.

- ExpressCard cellular modem (on ADSL models only)

  You can insert one ExpressCard cellular modem into the appliance's ExpressCard slot.

See ***Setting Up an ExpressCard Cellular Modem*** on page 185.

Setting Up an RS232 Modem

500 1000N

Note: Your RS232 dialup modem and your Safe@Office appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, refer to the *Embedded NGX CLI Reference Guide*.

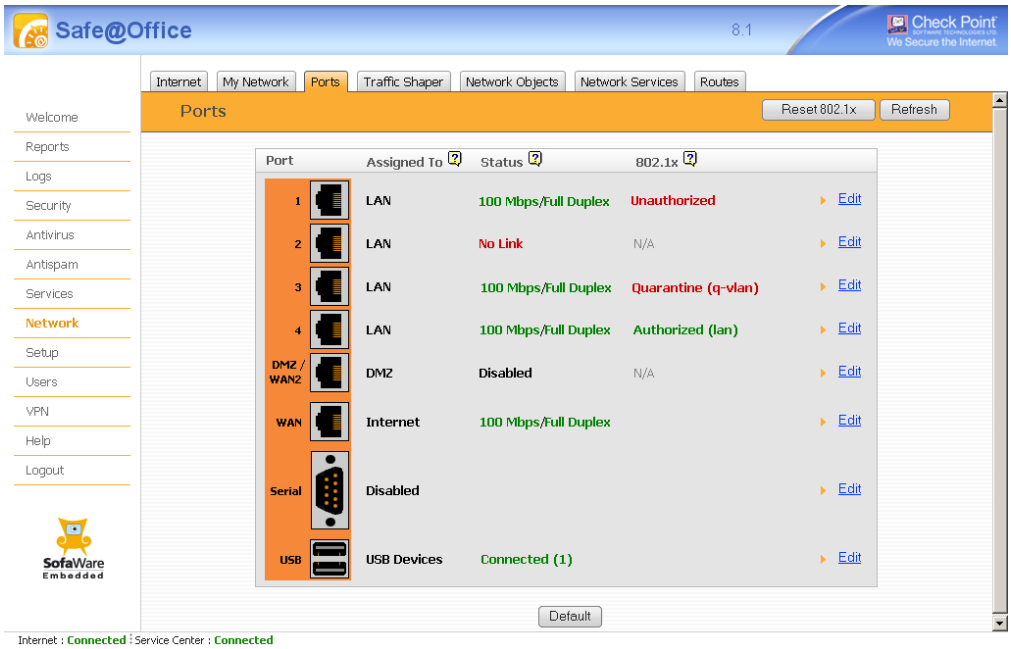
To set up an RS232 dialup modem

1. Connect an RS232 dialup modem to your Safe@Office appliance's serial port.

   For information on locating the serial port, see ***Introduction*** on page 1.

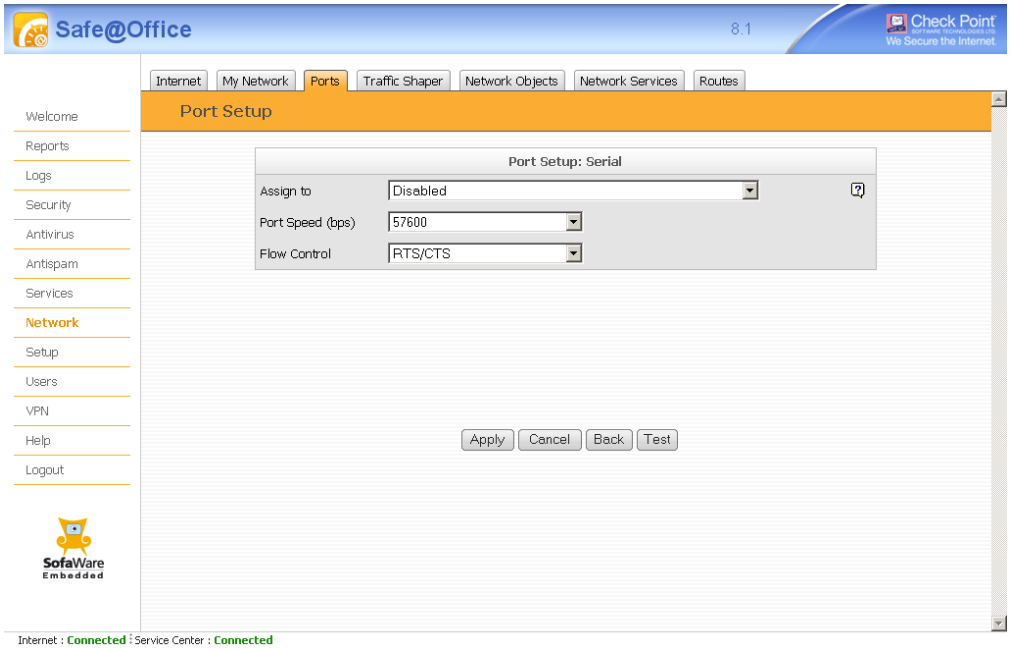
2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.



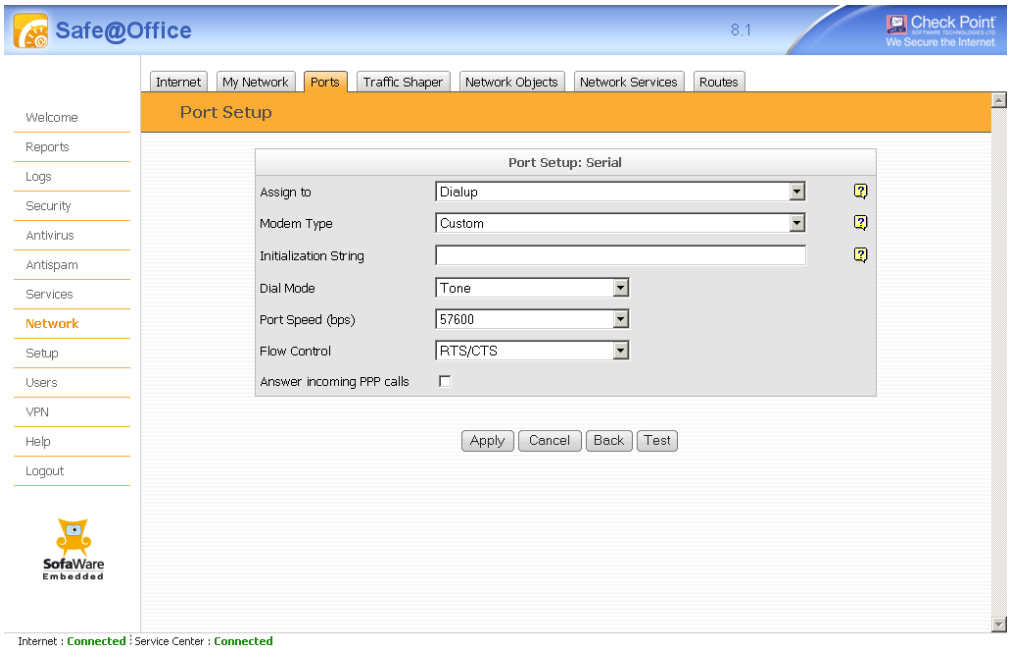
3. Next to **Serial**, click **Edit**.

   The **Port Setup** page appears.



4. In the **Assign to Network** drop-down list, select **Dialup**.

New fields appear.



5. Complete the fields using the information in ***Dialup Fields*** on page 180.
6. Click Apply.
7. To check that that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.
8. Configure a Dialup Internet connection on the Serial port.

   See ***Using Internet Setup*** on page 141.

Table 35: RS232 Dialup Fields

In this field…	Do this…
Modem Type	Select the modem type. You can select one of the predefined modem types or Custom. If you selected Custom, the Installation String field is enabled. Otherwise, it is filled in with the correct installation string for the modem type.
Initialization String	Type the installation string for the custom modem type. If you selected a standard modem type, this field is read-only.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the Serial port's speed (in bits per second). The Serial port's speed must match that of the attached dialup modem. The default value is 57600.
Flow Control	Select the method of flow control supported by the attached device: • RTS/CTS. Hardware-based flow control, using the Serial port's RTS/CTS lines. • XON/XOFF. Software-based flow control, using XON/XOFF characters.
Answer incoming PPP calls	Select this option to specify that the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***Configuring the OfficeMode Network*** on page 214.

Setting Up a USB Modem

USB

Warning: Before attaching a USB modem, ensure that the total power drawn by all connected USB devices does not exceed 2.5W per port (0.5A at 5V). If the total current consumed by a port exceeds 0.5A, a powered USB hub must be used, to avoid damage to the gateway.

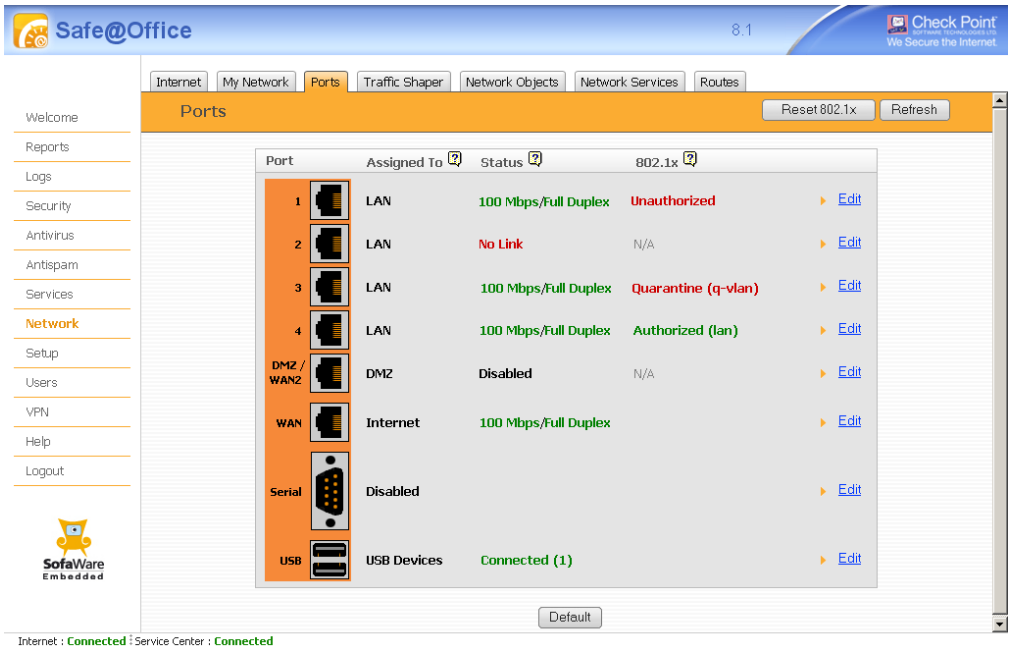
To set up a USB modem

1. Connect a USB-based modem to one of your Safe@Office appliance's USB ports.

   For information on locating the USB ports, see ***Introduction*** on page 1.

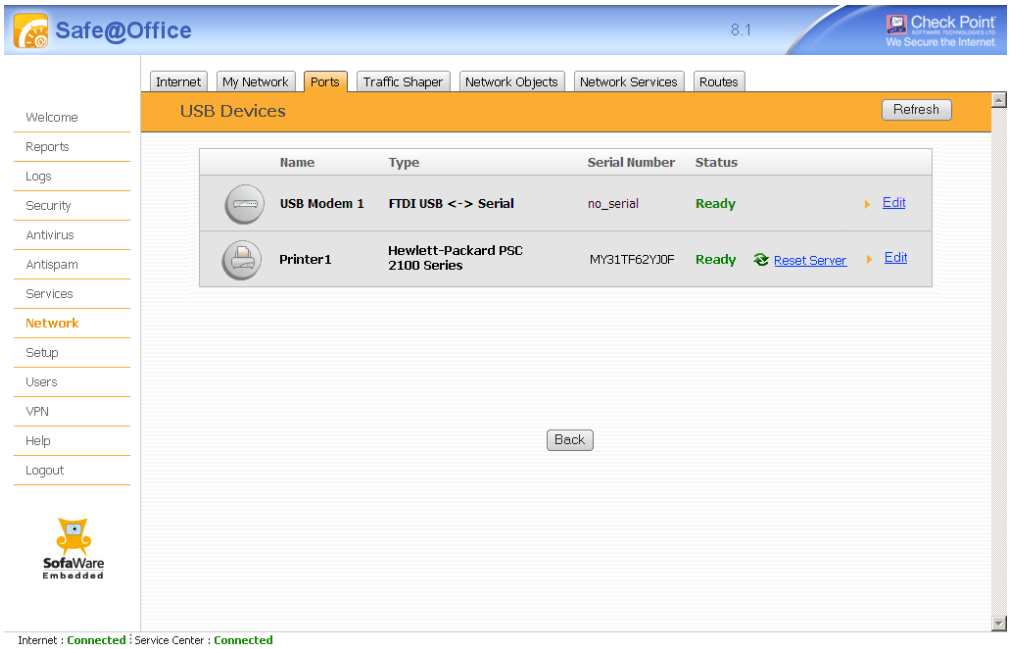
2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.



3. Next to USB, click Edit.

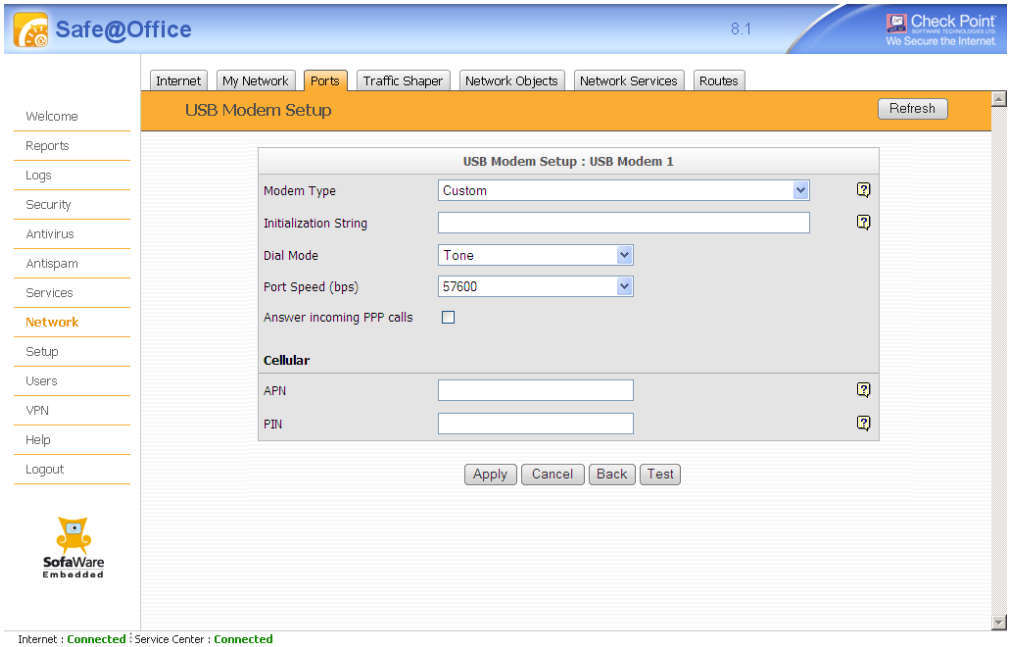
   The USB Devices page appears. If the Safe@Office appliance detected the modem, the modem is listed on the page.



   If the modem is not listed, check that you connected the modem correctly, then click Refresh to refresh the page.

4. Next to the modem, click Edit.

The USB Modem Setup page appears.



5. Complete the fields using the information in ***USB Dialup Fields*** on page 184.
6. Click Apply.
7. To check that that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.
8. Configure a Dialup Internet connection on the Cellular Modem port.

   See ***Using Internet Setup*** on page 141.

Table 36: USB Dialup Fields

In this field...	Do this...
Modem Type	Select the modem type. You can select one of the predefined modem types or Custom. If you selected Custom, the Installation String field is enabled. Otherwise, it is filled in with the correct installation string for the modem type.
Initialization String	Type the installation string for the custom modem type. If you selected a standard modem type, this field is read-only.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the modem's port speed (in bits per second).
Answer incoming PPP calls	Select this option to specify that the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***Configuring the OfficeMode Network*** on page 214.
Cellular	
APN	Type your Access Point Name (APN) as given by your cellular provider. If your cellular provider has not provided you with an APN, leave this field empty.

In this field...	Do this...
PIN	Type the Personal Identification Number (PIN) code that you received with your cellular SIM card, if required by your modem. The PIN code is usually 4 digits long. Warning: Entering an incorrect PIN code may cause your SIM card to be blocked.

Setting Up an ExpressCard Cellular Modem

ADSL

To set up an ExpressCard cellular modem

1. Insert an ExpressCard into the ExpressCard slot on the side of the appliance.

   For information on locating the ExpressCard slot, see ***Introduction*** on page 1.
2. Click Network in the main menu, and click the Ports tab.

The Ports page appears.

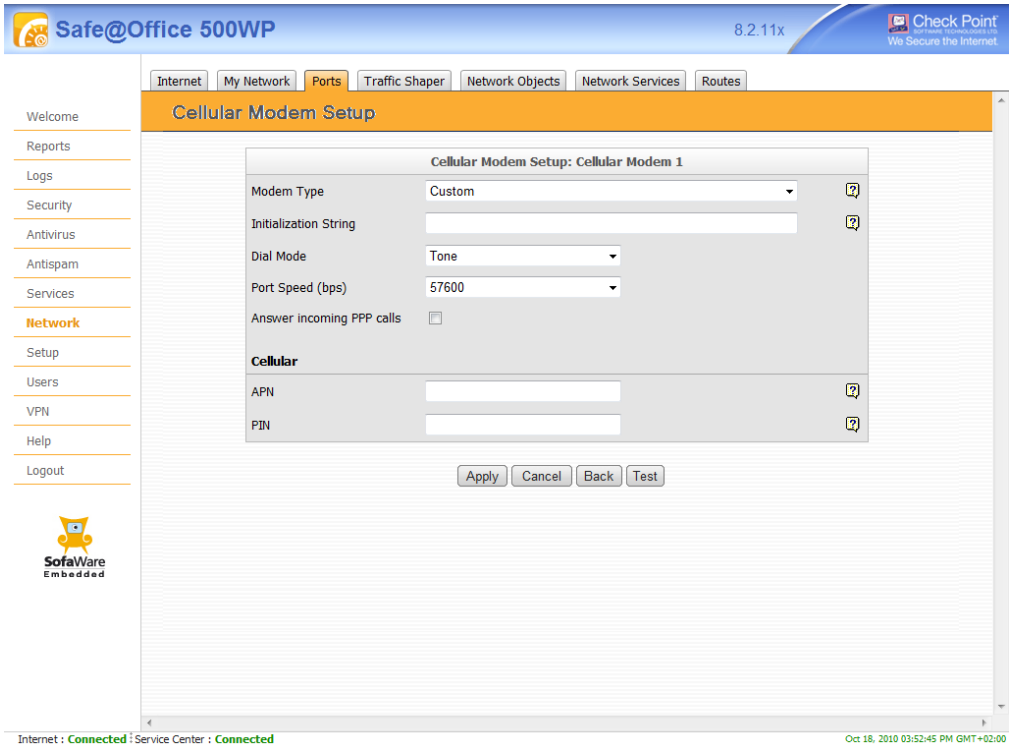
3. Next to ExC, click Edit.

   The USB Devices page appears. If the Safe@Office appliance detected the modem, the modem is listed on the page.

   If the modem is not listed, check that you connected the modem correctly, then click Refresh to refresh the page.

4. Next to the modem, click Edit.

The Cellular Modem Setup page appears.



5. Complete the fields using the information in ***USB Dialup Fields*** on page 184.
6. Click Apply.
7. To check that that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.
8. Configure a Dialup Internet connection on the Cellular Modem port.

   See ***Using Internet Setup*** on page 141.

Viewing Internet Connection Information

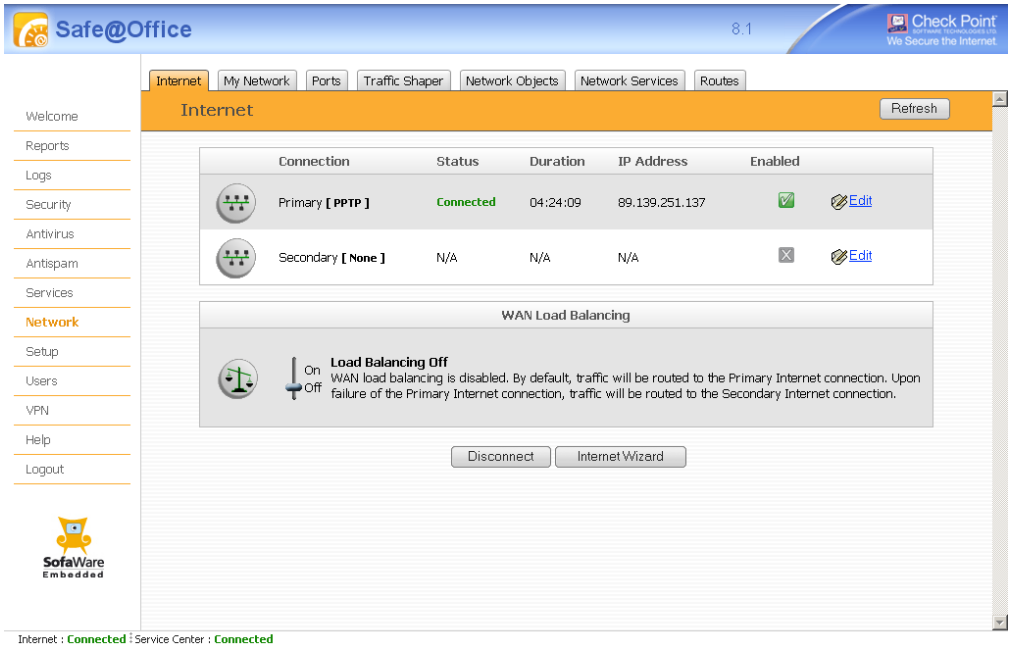
500 1000N

You can view information on your Internet connection(s) in terms of status, duration, and activity.

To view Internet connection information

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.



   For an explanation of the fields on this page, see the following table.

2. To refresh the information on this page, click Refresh.

Table 37: Internet Page Fields

Field	Description
Status	Indicates the connection's status.
Duration	Indicates the connection duration, if active. The duration is given in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds
IP Address	Your IP address.
Enabled	Indicates whether or not the connection is enabled. For further information, see ***Enabling/Disabling the Internet Connection*** on page 190

Enabling/Disabling the Internet Connection

500 1000N

You can temporarily disable an Internet connection. This is useful if, for example, you are going on vacation and do not want to leave your computer connected to the Internet. If you have two Internet connections, you can force the Safe@Office appliance to use a particular connection, by disabling the other connection.

The Internet connection's Enabled/Disabled status is persistent through Safe@Office appliance reboots.

To enable/disable an Internet connection

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

2. Next to the Internet connection, do one of the following:

   - To enable the connection, click .

     The button changes to and the connection is enabled.

   - To disable the connection, click .

     The button changes to and the connection is disabled.

Using Quick Internet Connection/Disconnection

500 1000N

By clicking the Connect or Disconnect button (depending on the connection status) on the Internet page, you can establish a quick Internet connection using the currently-selected connection type. In the same manner, you can terminate the active connection.

The Internet connection retains its Connected/Not Connected status until the Safe@Office appliance is rebooted. The Safe@Office appliance then connects to the Internet if the connection is enabled. For information on enabling an Internet connection, see ***Enabling/Disabling the Internet Connection*** on page 190.

Configuring a Backup Internet Connection

500 1000N

You can configure both a primary and a secondary Internet connection. The secondary connection acts as a backup, so that if the primary connection fails, the Safe@Office appliance remains connected to the Internet.

You have full flexibility in deciding which port to use for each Internet connection. You can assign the primary connection to use any of the following ports:

- WAN port (on Non-ADSL models)
- DSL port (on ADSL models)
- Serial port (for use with an RS232 modem)
- DMZ/WAN2 port
- USB ports (for use with a USB modem)
- ExpressCard slot

You can assign the secondary connection to use any of the above ports that is not being used by the primary connection.

Note: You can configure different DNS servers for the primary and secondary connections. The Safe@Office appliance acts as a DNS relay and routes requests from computers within the network to the appropriate DNS server for the active Internet connection.

Note: You can easily swap the roles of the primary and secondary connections, while simultaneously shifting all relevant port assignments between the primary and secondary connections, by using the swap wanconn CLI command. For information, refer to the *Embedded NGX CLI Reference Guide*.

Configuring WAN Load Balancing

500 1000N

If your network is prone to congestion, for example in large offices which include multiple active clients and/or servers, you can increase the amount of available bandwidth by configuring WAN load balancing. By default, the Safe@Office appliance routes all traffic to the primary Internet connection, and the secondary Internet connection is used only when the primary connection is down, or when a routing rule specifically states that traffic should be sent through the secondary connection. WAN load balancing automatically distributes traffic between the primary and secondary connections, allowing you to use both connections in parallel.

When one IP address sends packets to another IP address, the Safe@Office appliance examines each Internet connection's recent bandwidth utilization in kilobits per second to determine its load. The Safe@Office appliance then enters the source-destination pair in a load balancing table and specifies the least-loaded Internet connection as the connection to use for traffic between this pair. To prevent disruption of stateful protocols, the Safe@Office appliance will route *all* traffic between this pair to the specified Internet connection, so long as the pair remains in the load balancing table.

Note: By default, load balancing is performed when the amount of bandwidth utilization exceeds a threshold of 64 kilobits per second. You can change this threshold via the CLI. For information, refer to the Embedded NGX CLI Guide.

Note: By default, a source-destination pair is removed from the load balancing table after 1 hour of inactivity. You can change the default value via the CLI. For information, refer to the *Embedded NGX CLI Guide*.

Note: In order for WAN load balancing to be effective, there must be more than one active source-destination pair.

By default, the load distribution between Internet connections is symmetric; however, you can configure non-symmetric load balancing by assigning a different load balancing weight to each Internet connection. For example, if you assign the primary connection a weight of 100, and you assign the secondary connection a weight of 50, the Safe@Office appliance will only route traffic to the secondary connection if the primary connection's current load is more than twice the secondary connection's current load. Therefore, to

ensure full utilization of both Internet connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths.

Note: To ensure continuous Internet connectivity, if one of the Internet connections fails, all traffic will be routed to the other connection.

To configure WAN load balancing

1. Configure the desired load balancing weight for both the primary and secondary Internet connections.

   For further information, see the Load Balancing Weight field in ***Using Internet Setup*** on page 141.

2. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

3. In the WAN Load Balancing area, drag the load balancing lever to On.

   WAN load balancing is enabled. Traffic will be distributed automatically across the defined Internet connections, according to the configured load balancing weights.

Note: You can view the effect of WAN load balancing in the Traffic Monitor.

Chapter 6

Managing Your Network

This chapter describes how to manage and configure your network connection and settings.

This chapter includes the following topics:

Configuring Network Settings....195
Using the Internal DNS Server....224
Using Network Objects....227
Configuring Network Service Objects....237
Using Static Routes....241
Managing Ports....246

Configuring Network Settings

Note: If you accidentally change the network settings to incorrect values and are unable to connect to the my.firewall Web portal, you can connect to the appliance through the serial console and correct the error (see ***Using a Console*** on page *714*). Alternatively, you can reset the Safe@Office appliance to its default settings (see ***Resetting the Safe@Office appliance to Defaults*** on page *762*).

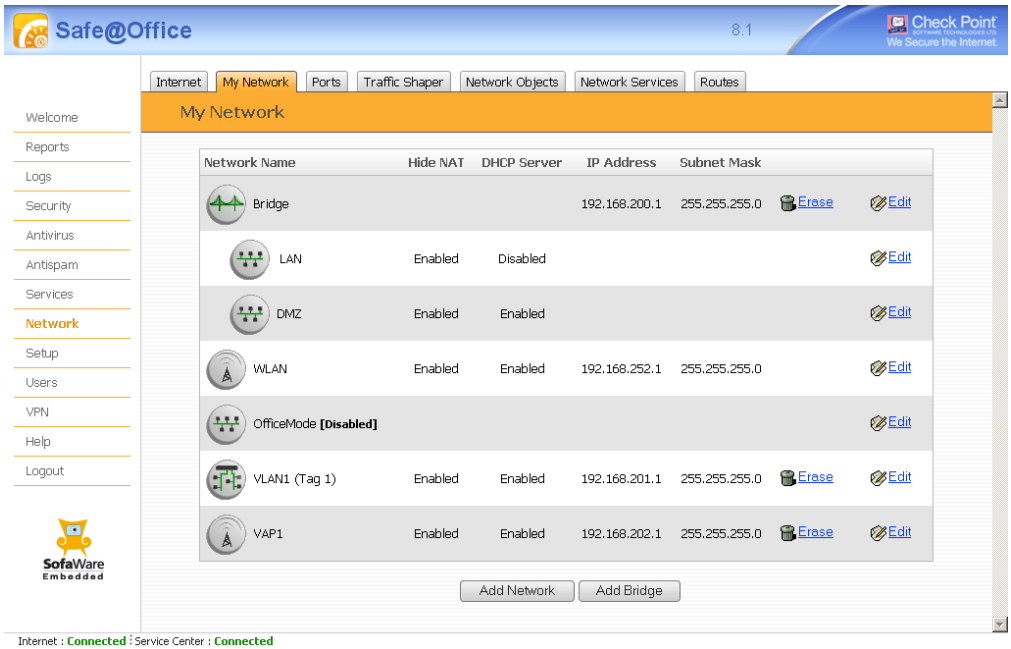
Configuring the LAN Network

500 1000N

To configure the LAN network

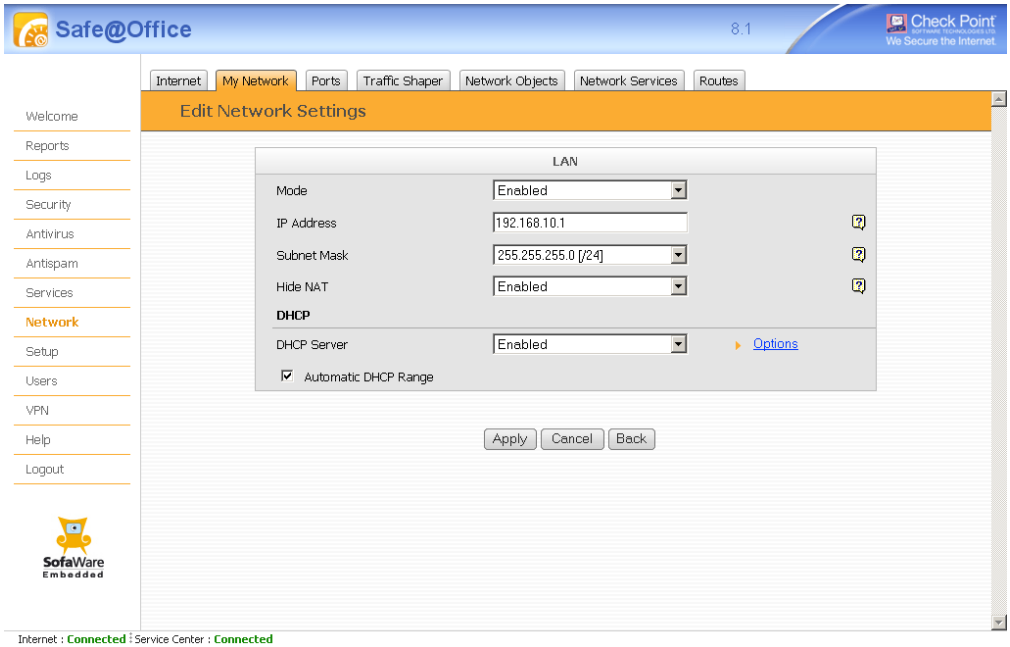
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.



2. Click Edit in the LAN network's row.

The Edit Network Settings page for the LAN network appears.



3. In the Mode drop-down list, select Enabled.

   The fields are enabled.

4. If desired, change your Safe@Office appliance's internal IP address.

   See ***Changing IP Addresses*** on page 198.

5. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 199.

6. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 200.

7. Click Apply.

   A warning message appears.

8. Click OK.

   A success message appears.

Changing IP Addresses

500 1000N

If desired, you can change your Safe@Office appliance's internal IP address, or the entire range of IP addresses in your internal network.

To change IP addresses

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. To change the Safe@Office appliance's internal IP address, enter the new IP address in the IP Address field.

4. To change the internal network range, enter a new value in the Subnet Mask field.

Note: The internal network range is defined both by the Safe@Office appliance's internal IP address and by the subnet mask.

For example, if the Safe@Office appliance's internal IP address is 192.168.100.7, and you set the subnet mask to 255.255.255.0, the network's IP address range will be 192.168.100.1 – 192.168.100.254.

5. Click Apply.

   A warning message appears.

6. Click OK.

   - The Safe@Office appliance's internal IP address and/or the internal network range are changed.
   - A success message appears.

7. Do one of the following:

   - If your computer is configured to obtain its IP address automatically (using DHCP), and the Safe@Office DHCP server is enabled, restart your computer.

Your computer obtains an IP address in the new range.

- Otherwise, manually reconfigure your computer to use the new address range using the TCP/IP settings. For information on configuring TCP/IP, see ***TCP/IP Settings*** on page 94.

Enabling/Disabling Hide NAT

500 1000N

Hide Network Address Translation (Hide NAT) enables you to share a single public Internet IP address among several computers, by "hiding" the private IP addresses of the internal computers behind the Safe@Office appliance's single Internet IP address.

Note: If Hide NAT is disabled, you must obtain a range of Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT, Hide NAT, and custom NAT rules can be used together.

To enable/disable Hide NAT

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. From the Hide NAT list, select Enabled or Disabled.
4. Click Apply.

   A warning message appears.

5. Click OK.
   - If you chose to disable Hide NAT, it is disabled.
   - If you chose to enable Hide NAT, it is enabled.

Configuring a DHCP Server

500 1000N

By default, the Safe@Office appliance operates as a DHCP (Dynamic Host Configuration Protocol) server. This allows the Safe@Office appliance to automatically configure all the devices on your network with their network configuration details.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. However, if you do assign the computer an IP address within the DHCP address range, the DHCP server will detect this and will not assign this IP address to another computer.

If you already have a DHCP server in your internal network, and you want to use it instead of the Safe@Office DHCP server, you must disable the Safe@Office DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Safe@Office DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Safe@Office appliance relays information from the desired DHCP server to the devices on your network.

Note: You can perform DHCP reservation using network objects. For information, see ***Using Network Objects*** on page *227*.

Note: The following DHCP server configurations are not available for the OfficeMode network:

- Enabling and disabling the Safe@Office DHCP Server
- Setting the DHCP range manually
- Configuring DHCP relay

Enabling/Disabling the Safe@Office DHCP Server

500 1000N

You can enable and disable the Safe@Office DHCP Server for internal networks.

To enable/disable the Safe@Office DHCP server

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. From the DHCP Server list, select Enabled or Disabled.

4. Click Apply.

   A warning message appears.

5. Click OK.

   A success message appears

6. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   If you enabled the DHCP server, your computer obtains an IP address in the DHCP address range.

Configuring the DHCP Address Range

500 1000N

By default, the Safe@Office DHCP server automatically sets the DHCP address range. The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

If desired, you can set the Safe@Office DHCP range manually.

To configure the DHCP address range

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

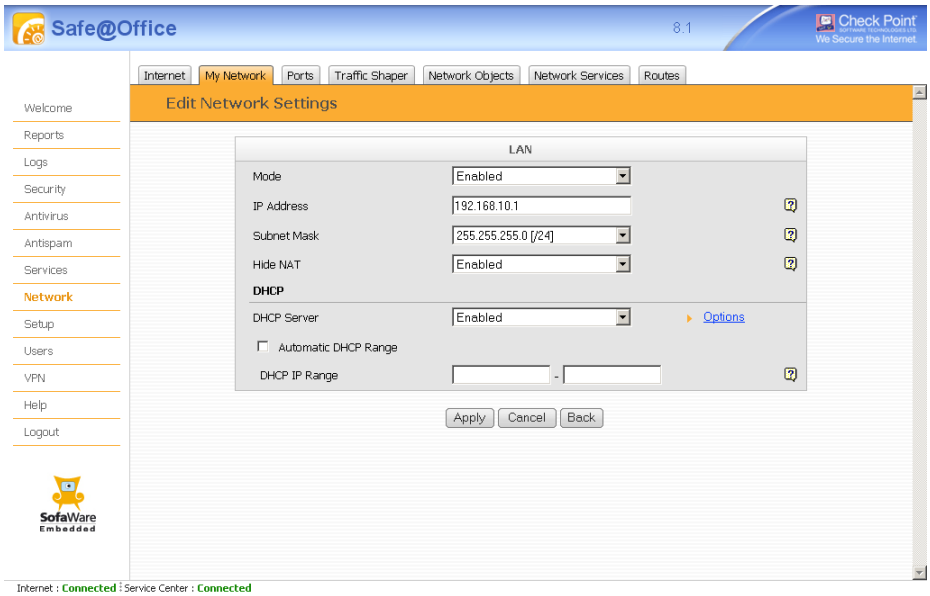
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. Do one of the following:

   - To allow the DHCP server to set the IP address range, select the Automatic DHCP range check box.
   - To set the DHCP range manually:
     1) Clear the Automatic DHCP range check box.

The DHCP IP range fields appear.



2) In the DHCP IP range fields, type the desired DHCP range.

4. Click Apply.

   A warning message appears.

5. Click OK.

   A success message appears

6. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   Your computer obtains an IP address in the new DHCP address range.

Configuring DHCP Relay

500 1000N

You can configure DHCP relay for internal networks.

Note: DHCP relay will not work if the appliance is located behind a NAT device.

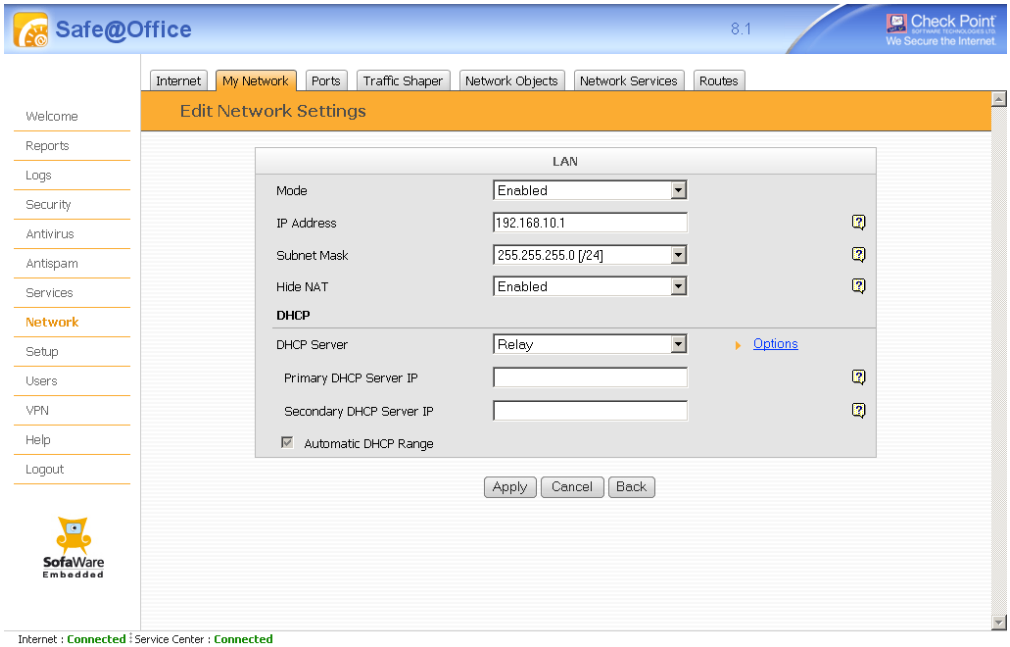
To configure DHCP relay

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.
3. In the DHCP Server list, select Relay.

The Automatic DHCP range check box is disabled, and new fields appear.



4. In the Primary DHCP Server IP field, type the IP address of the primary DHCP server.
5. In the Secondary DHCP Server IP field, type the IP address of the DHCP server to use if the primary DHCP server fails.
6. Click Apply.

   A warning message appears.
7. Click OK.

   A success message appears
8. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   Your computer obtains an IP address in the DHCP address range.

Configuring DHCP Server Options

500 1000N

If desired, you can configure the following custom DHCP options for an internal network:

- Domain suffix
- DNS servers
- WINS servers
- Default gateway
- NTP servers
- VoIP call managers
- TFTP server and boot filename
- Avaya, Nortel, and Thomson IP phone configuration strings

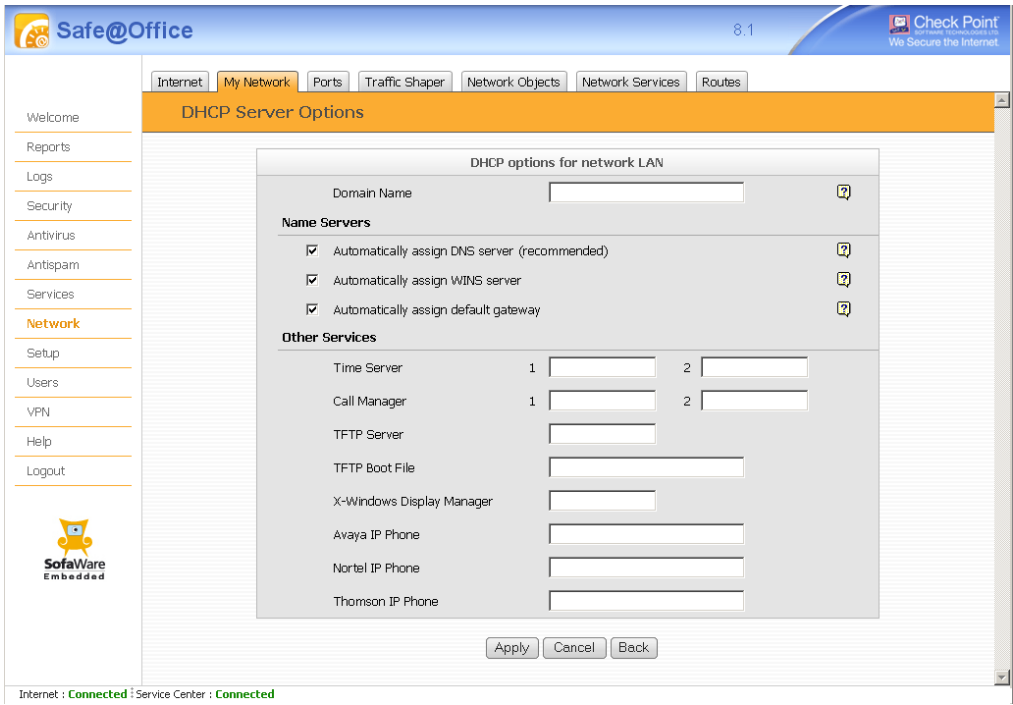
To configure DHCP options

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
2. In the desired network's row, click Edit.

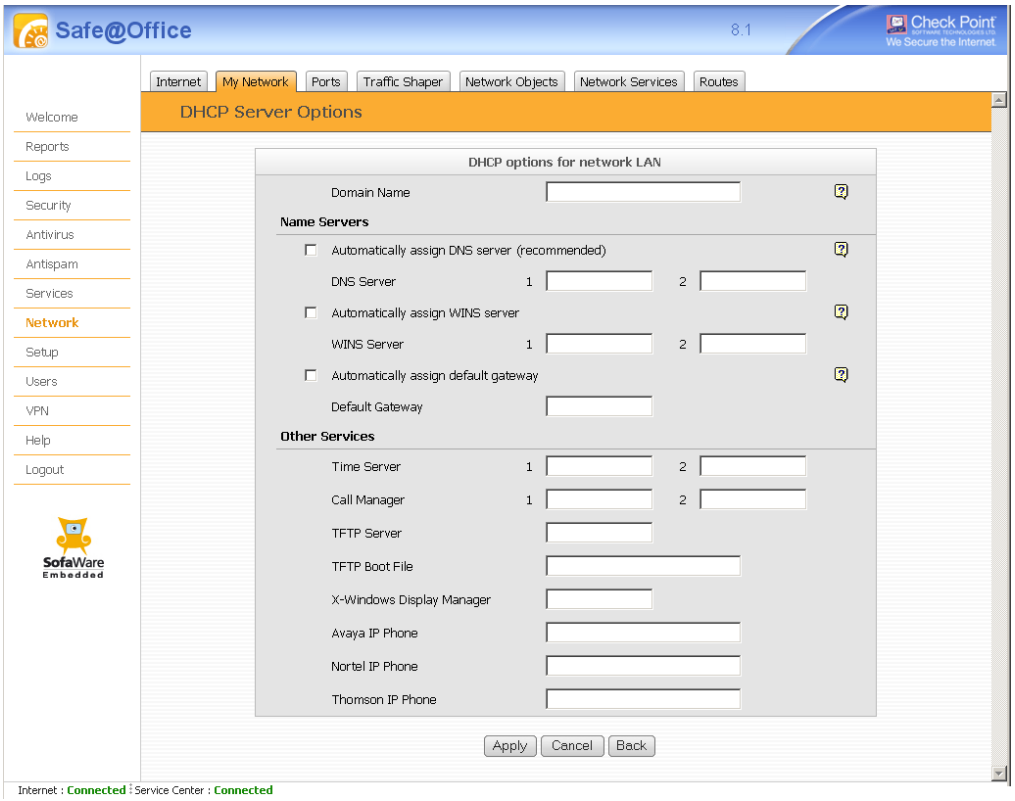
   The Edit Network Settings page appears.
3. In the DHCP area, click Options.

The DHCP Server Options page appears.



4. Complete the fields using the relevant information in the following table.

New fields appear, depending on the check boxes you selected.



5. Click Apply.
6. If your computer is configured to obtain its IP address automatically (using DHCP), restart your computer.

   Your computer obtains an IP address in the DHCP address range.

Table 38: DHCP Server Options Fields

In this field…	Do this…
Domain Name	Type a default domain suffix that should be passed to DHCP clients. The DHCP client will automatically append the domain suffix for the resolving of non-fully qualified names. For example, if the domain suffix is set to "mydomain.com", and the client tries to resolve the name “mail”, the suffix will be automatically appended to the name, resulting in “mail.mydomain.com”.
Name Servers	
Automatically assign DNS server (recommended)	Clear this option if you do not want the gateway to act as a DNS relay server and pass its own IP address to DHCP clients. Normally, it is recommended to leave this option selected. The DNS Server 1 and DNS Server 2 fields appear.
DNS Server 1, 2	Type the IP addresses of the Primary and Secondary DNS servers to pass to DHCP clients instead of the gateway.
Automatically assign WINS server	Clear this option if you do not want DHCP clients to be assigned the same WINS servers as specified by the Internet connection configuration (in the Internet Setup page). The WINS Server 1 and WINS Server 2 fields appear.
WINS Server 1, 2	Type the IP addresses of the Primary and Secondary WINS servers to use instead of the gateway.

In this field...	Do this...
Automatically assign default gateway	Clear this option if you do not want the DHCP server to pass the current gateway IP address to DHCP clients as the default gateway's IP address. Normally, it is recommended to leave this option selected. The Default Gateway field is enabled.
Default Gateway	Type the IP address to pass to DHCP clients as the default gateway, instead of the current gateway IP address.
Other Services	These fields are not available for the OfficeMode network.
Time Server 1, 2	To use Network Time Protocol (NTP) servers to synchronize the time on the DHCP clients, type the IP address of the Primary and Secondary NTP servers.
Call Manager 1, 2	To assign Voice over Internet Protocol (VoIP) call managers to the IP phones, type the IP address of the Primary and Secondary VoIP servers.
TFTP Server	Trivial File Transfer Protocol (TFTP) enables booting diskless computers over the network. To assign a TFTP server to the DHCP clients, type the IP address of the TFTP server.
TFTP Boot File	Type the boot file to use for booting DHCP clients via TFTP.
X-Windows Display Manager	To assign X-Windows terminals the appropriate X-Windows Display Manager when booting via DHCP, type the XDM server's IP address.
Avaya IP Phone	To enable Avaya IP phones to receive their configuration, type the phone's configuration string.

In this field...	Do this...
Nortel IP Phone	To enable Nortel IP phones to receive their configuration, type the phone's configuration string.
Thomson IP Phone	To enable Thomson IP phones to receive their configuration, type the phone's configuration string.

Configuring a DMZ Network

500 1000N

In addition to the LAN network, you can define a second internal network called a DMZ (demilitarized zone) network.

For information on default security policy rules controlling traffic to and from the DMZ, see ***Default Security Policy*** on page 393.

To configure a DMZ network

1. Connect the DMZ computer to the DMZ port.

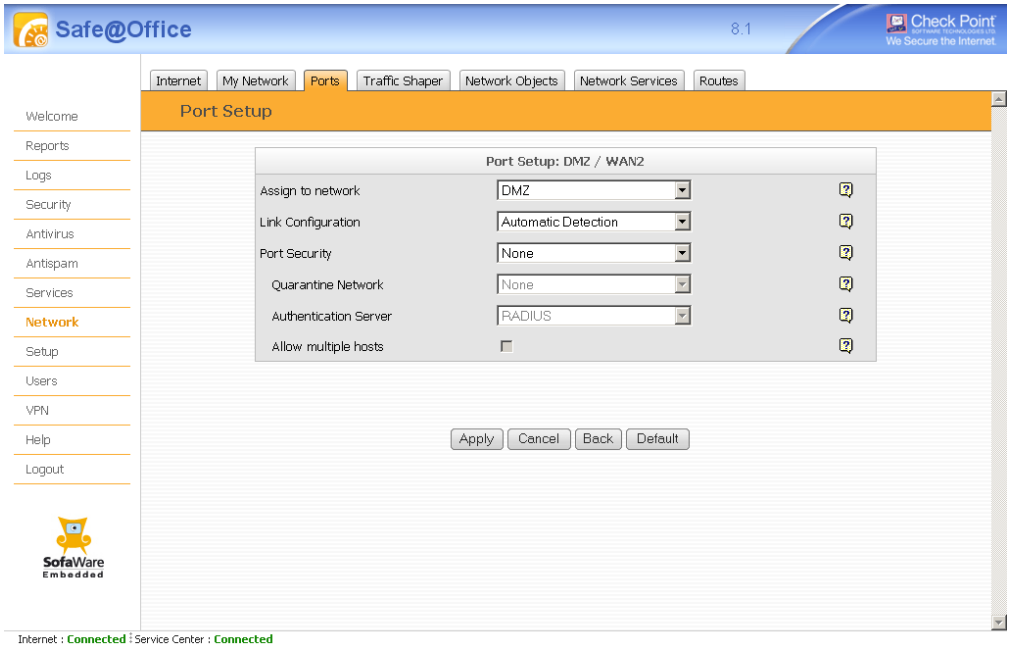
   If you have more than one computer in the DMZ network, connect a hub or switch to the DMZ port, and connect the DMZ computers to the hub.

2. Click Network in the main menu, and click the Ports tab.

The Ports page appears.

3. Next to the DMZ/WAN2 port, click Edit.

The Port Setup page appears.



4. In the Assign to network drop-down list, select DMZ.
5. Click Apply.

   A warning message appears.
6. Click OK.
7. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
8. In the DMZ network's row, click Edit.

   The Edit Network Settings page appears.
9. In the Mode drop-down list, select Enabled.

   The fields are enabled.
10. In the IP Address field, type the IP address of the DMZ network's default gateway.

Note: The DMZ network must not overlap other networks.

11. In the Subnet Mask drop-down list, select the DMZ's internal network range.
12. If desired, enable or disable Hide NAT.

    See ***Enabling/Disabling Hide NAT*** on page 199.
13. If desired, configure a DHCP server.

    See ***Configuring a DHCP Server*** on page 200.
14. Click Apply.

    A warning message appears.
15. Click OK.

    A success message appears.

Configuring the OfficeMode Network

500 1000N

By default, VPN Clients connect to the VPN Server using an Internet IP address locally assigned by an ISP. This may lead to the following problems:

- VPN Clients on the same network will be unable to communicate with each other via the Safe@Office Internal VPN Server. This is because their IP addresses are on the same subnet, and they therefore attempt to communicate directly over the local network, instead of through the secure VPN link.
- Some networking protocols or resources may require the client's IP address to be an internal one.

OfficeMode solves these problems by enabling the Safe@Office DHCP Server to automatically assign a unique local IP address to the VPN client, when the client connects and authenticates. The IP addresses are allocated from a pool called the *OfficeMode network*.

Note: OfficeMode requires either Check Point SecureClient, an L2TP client, or an Endpoint Connect client to be installed on the VPN clients. It is not supported by Check Point SecuRemote.

When OfficeMode is not supported by the VPN client, traditional mode will be used instead.

To configure the OfficeMode network

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the OfficeMode network's row, click Edit.

   The Edit Network Settings page appears.

3. In the Mode drop-down list, select Enabled.

   The fields are enabled.

4. In the IP Address field, type the IP address to use as the OfficeMode network's default gateway.

Note: The OfficeMode network must not overlap other networks.

5. In the Subnet Mask text box, type the OfficeMode internal network range.
6. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 199.

7. If desired, configure DHCP options.

   See ***Configuring DHCP Server Options*** on page 206.

8. Click Apply.

   A warning message appears.

9. Click OK.

   A success message appears.

Configuring VLANs

500 | 1000N | Power Pack

Your Safe@Office appliance allows you to partition your network into several virtual LAN networks (VLANs). A VLAN is a logical network behind the Safe@Office appliance. Computers in the same VLAN behave as if they were on the same physical network: traffic flows freely between them, without passing through a firewall. In contrast, traffic between a VLAN and other networks passes through the firewall and is subject to the security policy. By default, traffic from a VLAN to any other internal network (including other VLANs) is blocked. In this way, defining VLANs can increase security and reduce network congestion.

For example, you can assign each division within your organization to a different VLAN, regardless of their physical location. The members of a division will be able to communicate with each other and share resources, and only members who need to communicate with other divisions will be allowed to do so. Furthermore, you can easily transfer a member of one division to another division without rewiring your network, by simply reassigning them to the desired VLAN.

The Safe@Office appliance supports the following VLAN types:

- Tag-based

  In tag-based VLAN you use one of the gateway's ports as a 802.1Q VLAN trunk, connecting the appliance to a VLAN-aware switch. Each VLAN behind the trunk is assigned an identifying number called a "VLAN ID", also referred to as a "VLAN tag". All outgoing traffic from a tag-based VLAN contains the VLAN's tag in the packet headers. Incoming traffic to the VLAN must contain the VLAN's tag as well, or the packets are dropped. Tagging ensures that traffic is directed to the correct VLAN.

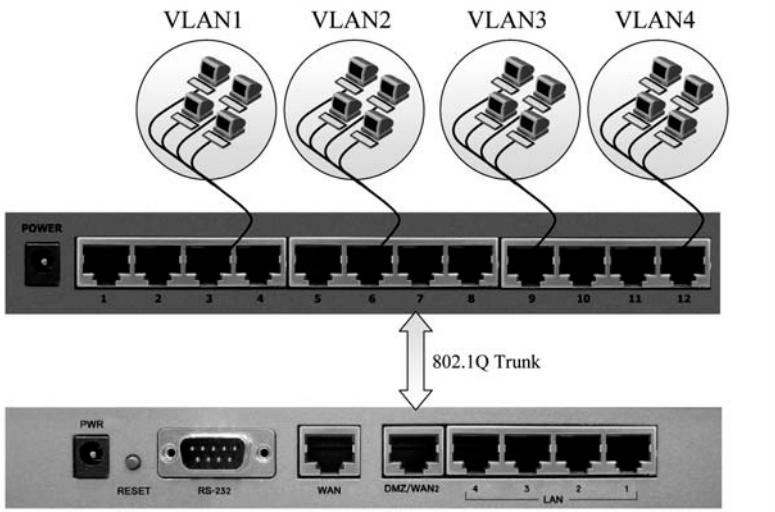


Figure 27: Tag-Based VLAN

- Port-based

  Port-based VLAN allows assigning the appliance's LAN ports to VLANs, effectively transforming the appliance's four-port switch into up to four firewall-isolated security zones. You can assign multiple ports to the same VLAN, or each port to a separate VLAN.

  Port-based VLAN does not require an external VLAN-capable switch, and is therefore simpler to use than tag-based VLAN. However, port-based VLAN is limited by the number of appliance LAN ports.

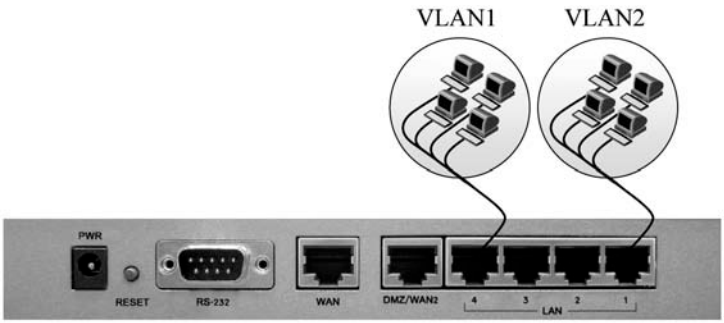


Figure 28: Port-Based VLAN

- Virtual access point (VAP)

  In wireless Safe@Office models, you can partition the primary WLAN network into wireless VLANs called virtual access points (VAPs). You can use VAPs to grant different permissions to groups of wireless users, by configuring each VAP with the desired security policy and network settings, and then assigning each group of wireless users to the relevant VAP. For example, you could assign different permissions to employees and guests on the company's wireless network, by configuring two VAPs called “Guest” and “Employee” with the desired set of permissions.

  To use VAPs, you must enable the primary WLAN network.

  For more information on VAPs, see ***Overview*** on page 305.

- Wireless Distribution System (WDS) links

  In wireless Safe@Office models, you can extend the primary WLAN's coverage area, by creating a Wireless Distribution System (WDS). A WDS is a system of access points that communicate with each other wirelessly, without any need for a wired backbone. WDS is usually used together with bridge mode to connect the networks behind the access points.

  To create a WDS, you must add WDS links between the desired access points. For example, if your business extends across a large area, and a single access point does not provide sufficient coverage, then you can add a second access point and create a WDS link between the two access points.

  To use WDS links, you must enable the primary WLAN network.

  For more information on WDS links, see ***Overview*** on page 305.

In Safe@Office models with unlimited nodes, you can define up to 64 VLAN networks (port-based, tag-based, VAP, and WDS links combined), while in other models, you can define up to ten VLAN networks. In wireless models, up to three of the VLAN networks can be VAPs, and up to seven of the VLAN networks can be WDS links. For information on counting VAPs and WDS links, see ***Configuring a Wireless Network*** on page 305.

For information on the default security policy for VLANs, see ***Default Security Policy*** on page 393.

Adding and Editing VLANs

Power Pack

For information on adding and editing port-based VLANs, see ***Adding and Editing Port-Based VLANs*** on page 220.

For information on adding and editing tag-based VLANs, see ***Adding and Editing Tag-Based VLANs*** on page 222.

For information on adding and editing VAPs, see ***Configuring Virtual Access Points*** on page 333.

For information on adding and editing WDS links, see ***Configuring WDS Links*** on page 338.

Adding and Editing Port-Based VLANs

Power Pack

To add or edit a port-based VLAN

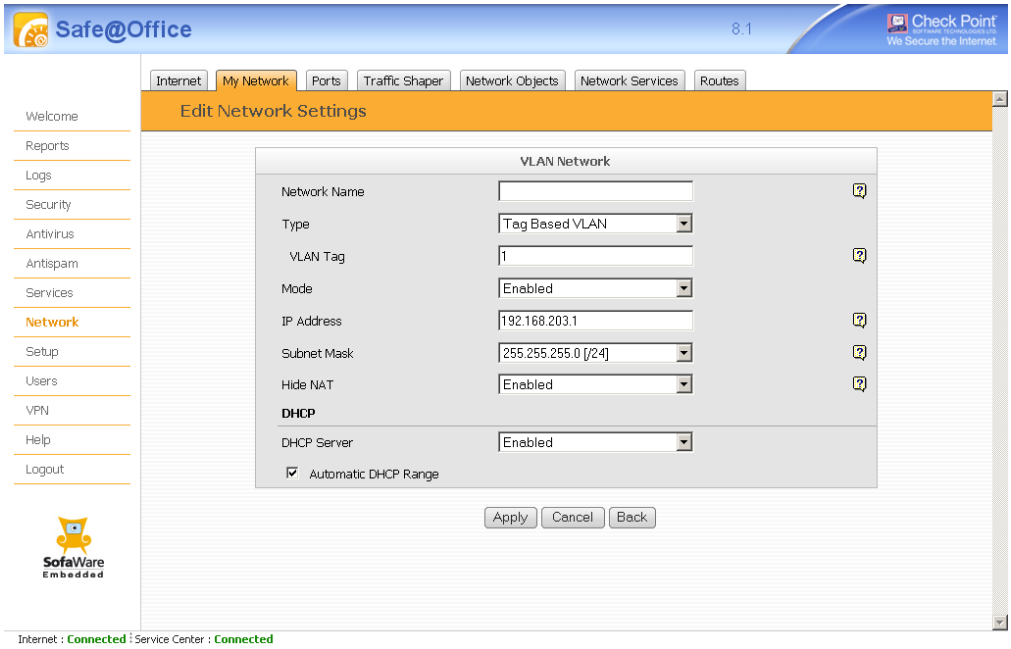
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Do one of the following:

   - To add a VLAN, click Add Network.
   - To edit a VLAN, click Edit in the desired VLAN's row.

   The Edit Network Settings page for VLAN networks appears.



3. In the Network Name field, type a name for the VLAN.
4. In the Type drop-down list, select Port Based VLAN.

   The VLAN Tag field disappears.

5. In the Mode drop-down list, select Enabled.

   The fields are enabled.

6. In the IP Address field, type the IP address of the VLAN network's default gateway.

Note: The VLAN network must not overlap other networks.

7. In the Subnet Mask field, type the VLAN's internal network range.
8. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 199.

9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 200.

10. Click Apply.

    A warning message appears.

11. Click OK.

    A success message appears.

12. Click Network in the main menu, and click the Ports tab.

    The Ports page appears.

13. Next to the LAN port you want to assign, click Edit.

    The Port Setup page appears.

14. In the Assign to network drop-down list, select the VLAN network's name.

    You can assign more than one port to the VLAN.

15. Click Apply.

Adding and Editing Tag-Based VLANs

Power Pack

To add or edit a tag-based VLAN

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Do one of the following:

   - To add a VLAN, click Add Network.
   - To edit a VLAN, click Edit in the desired VLAN's row.

   The Edit Network Settings page for VLAN networks appears.

3. In the Network Name field, type a name for the VLAN.
4. In the Type drop-down list, select Tag Based VLAN.

   The VLAN Tag field appears.

5. In the VLAN Tag field, type a tag for the VLAN.

   This must be an integer between 1 and 4095.

6. In the Mode drop-down list, select Enabled.

   The fields are enabled.

7. In the IP Address field, type the IP address of the VLAN network's default gateway.

Note: The VLAN network must not overlap other networks.

8. In the Subnet Mask field, type the VLAN's internal network range.
9. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 199.

10. If desired, configure a DHCP server.

    See ***Configuring a DHCP Server*** on page 200.

11. Click Apply.

A warning message appears.

12. Click OK.

    A success message appears.

13. Click Network in the main menu, and click the Ports tab.

    The Ports page appears.

14. In the DMZ/WAN2 drop-down list, select VLAN Trunk.

15. Click Apply.

    The DMZ/WAN2 port now operates as a VLAN Trunk port. In this mode, it will not accept untagged packets.

16. Configure a VLAN trunk (802.1Q) port on the VLAN-aware switch, according to the vendor instructions. Define the same VLAN IDs on the switch.

17. Connect the Safe@Office appliance's DMZ/WAN2 port to the VLAN-aware switch's VLAN trunk port.

Deleting VLANs

Power Pack

To delete a VLAN

1. If the VLAN is port-based, do the following:
   a. Click Network in the main menu, and click the Ports tab.

      The Ports page appears.

   b. Remove all port assignments to the VLAN, by selecting other networks in the drop-down lists.
   c. Click Apply.
2. Delete any firewall rules or VStream Antivirus rules that use this VLAN.
3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

4. In the desired VLAN's row, click Erase.

   A confirmation message appears.

5. Click OK.

   The VLAN is deleted.

Using the Internal DNS Server

500 1000N

The Safe@Office appliance includes an internal DNS server, which can resolve DNS names for hosts defined as network objects. Each host is assigned a DNS name in the format `<networkobjectname>.<domainsuffix>`, where `<networkobjectname>` is the name of the network object representing the host, and `<domainsuffix>` is the domain name suffix configured for the internal DNS server. The internal DNS server will reply to all DNS requests for the host's DNS name with the host's IP address.

In addition to resolving network objects, the internal DNS server also resolves requests for the current gateway. If a gateway hostname is defined, the DNS server will reply to DNS requests in the format `<hostname>.<domainsuffix>` with the gateway's internal IP address. For information on configuring the gateway's hostname, see ***Configuring a Gateway Hostname*** on page 724.

Note: The internal DNS server responds to DNS requests from internal network hosts only. It does not respond to requests from the Internet.

Example

If a computer with the IP address 192.188.22.1 is represented by a network object called "server1", and the internal DNS server is configured with the domain suffix "mycompany.com", then the computer's DNS name will be "server1.mycompany.com", and the internal DNS server will reply to all DNS requests for "server1.mycompany.com" with the IP address 192.188.22.1.

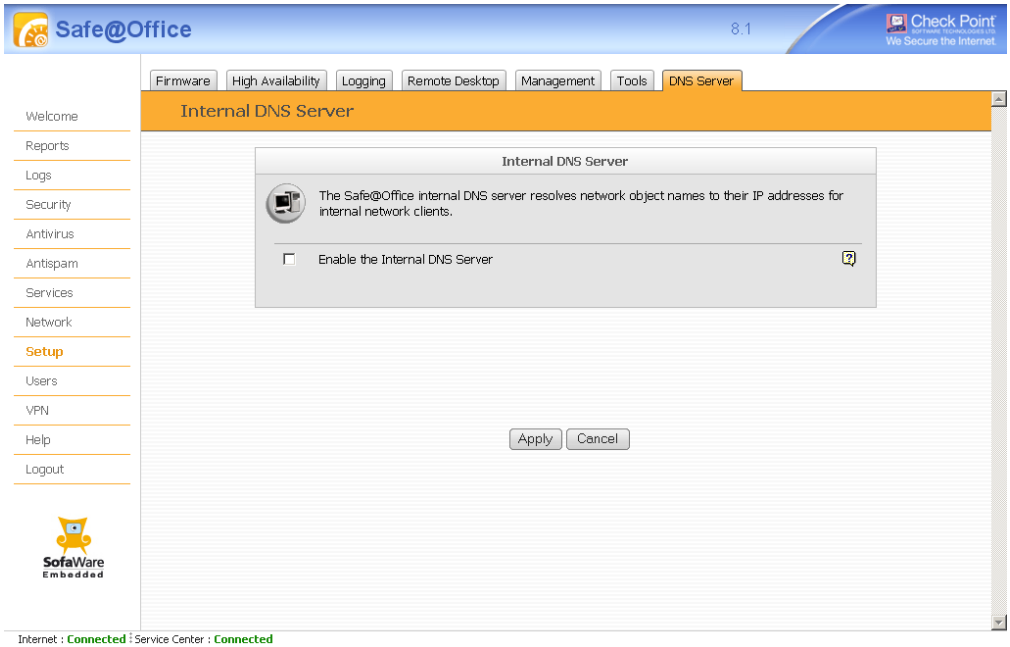
In addition, if the gateway is configured with the hostname "mygateway", the DNS server will reply to all DNS requests for "mygateway.mycompany.com" with the gateway's internal IP address.

Enabling the Internal DNS Server

To enable the internal DNS server

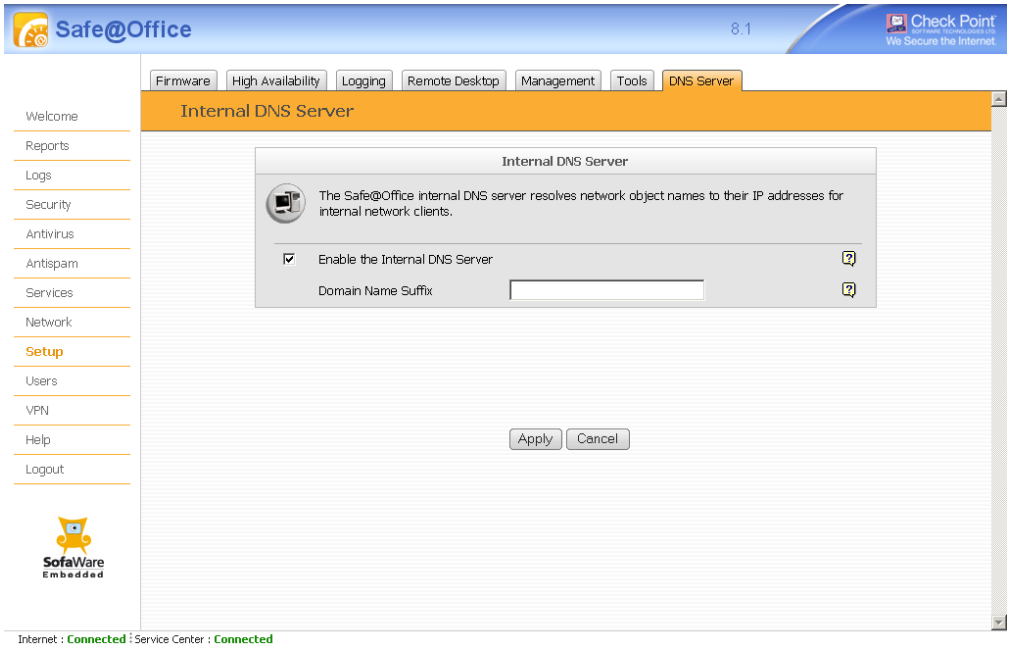
1. Click Setup in the main menu, and click the DNS Server tab.

   The DNS Server page appears.



2. Select the Enable the Internal DNS Server check box.

The Domain Name Suffix field appears.



3. In the Domain Name Suffix field, type the desired domain name suffix.
4. Click Apply.

Using Network Objects

500 1000N

You can add individual computers or networks as network objects. This enables you to configure various settings for the computer or network represented by the network object.

You can configure the following settings for a network object:

- Static NAT (or One-to-One NAT)

  Static NAT allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. This is useful if you want a computer in your private network to have its own Internet IP address. For example, if you have both a mail server and a Web server in your network, you can map each one to a separate Internet IP address.

  Static NAT rules do not imply any security rules. To allow incoming traffic to a host for which you defined Static NAT, you must create an Allow rule. When specifying firewall rules for such hosts, use the host's internal IP address, and not the Internet IP address to which the internal IP address is mapped. For further information, see ***Using Rules*** on page 400.

Note: Static NAT, Hide NAT, and custom NAT rules can be used together.

Note: The Safe@Office appliance supports Proxy ARP (Address Resolution Protocol). When an external source attempts to communicate with such a computer, the Safe@Office appliance automatically replies to ARP queries with its own MAC address, thereby enabling communication. As a result, the Static NAT Internet IP addresses appear to external sources to be real computers connected to the WAN interface.

- Assign the network object's IP address to a MAC address

  Normally, the Safe@Office DHCP server consistently assigns the same IP address to a specific computer. However, if the Safe@Office DHCP server runs out of IP addresses and the computer is down, then the DHCP server may reassign the IP address to a different computer.

  If you want to guarantee that a particular computer's IP address remains constant, you can reserve the IP address for use by the computer's MAC address only. This is called

DHCP reservation, and it is useful if you are hosting a public Internet server on your network.

- Web Filtering enforcement

  You can specify whether or not to enforce the Web Filtering service and Web rules for the network object. Network objects that are excluded from such enforcement will be able to access the Internet without restriction. For information on Web Filtering, see ***Web Filtering*** on page 575. For information on Web rules, see ***Using Web Rules*** on page 567.

- Secure HotSpot enforcement

  In Safe@Office products with Power Pack, you can specify whether or not to exclude the network object from HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access the excluded network object without viewing the My HotSpot page. For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 419.

- 802.1x port-based security enforcement

  In Safe@Office products with Power Pack, when DHCP reservation is used, you can specify whether or not to exclude a computer from 802.1x port-based security enforcement. Excluded computers will be able to connect to the Safe@Office appliance's ports and access the network without authenticating. For information on 802.1x port-based security, see ***Using Port-Based Security*** on page 413.

Adding and Editing Network Objects

500 1000N

You can add or edit network objects via:

- The Network Objects page

  This page enables you to add both individual computers and networks.

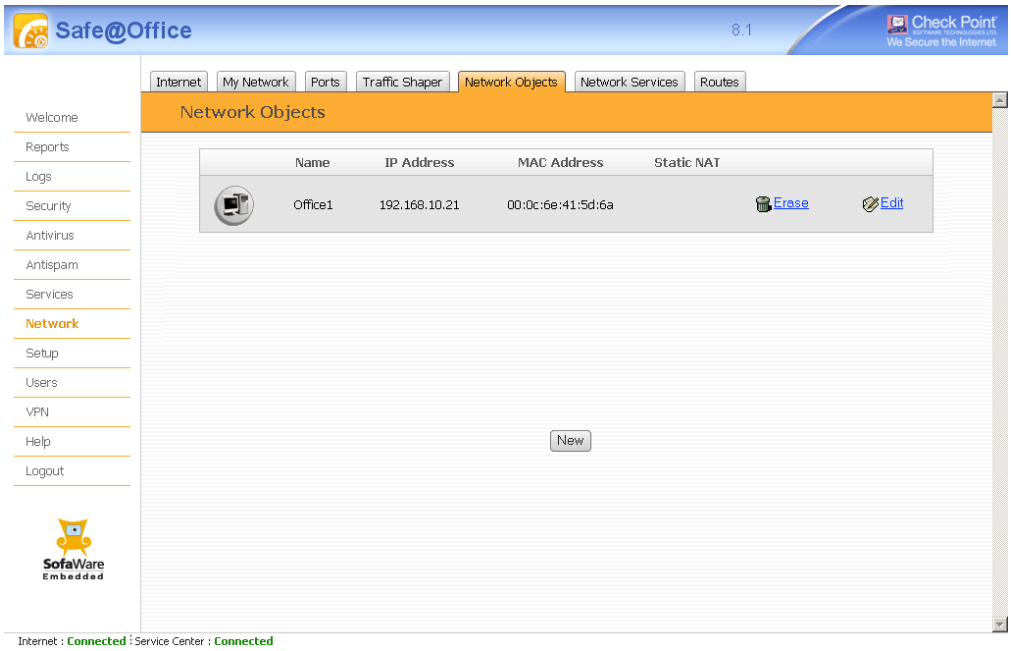
- The My Computers page

  This page enables you to add only individual computers as network objects. The computer's details are filled in automatically in the wizard.

To add or edit a network object via the Network Objects page

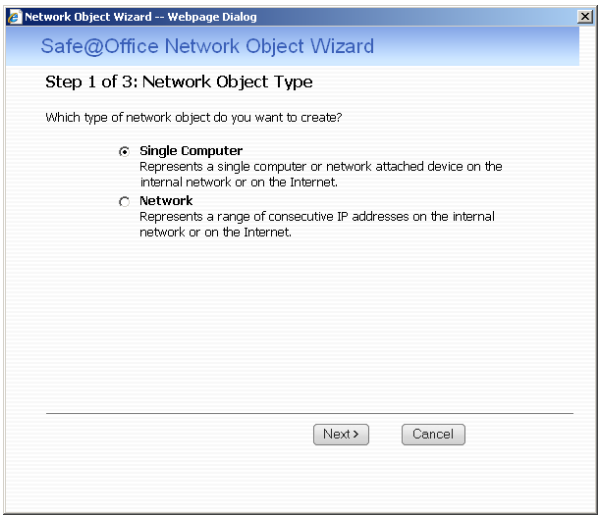
1. Click Network in the main menu, and click the Network Objects tab.

   The Network Objects page appears with a list of network objects.



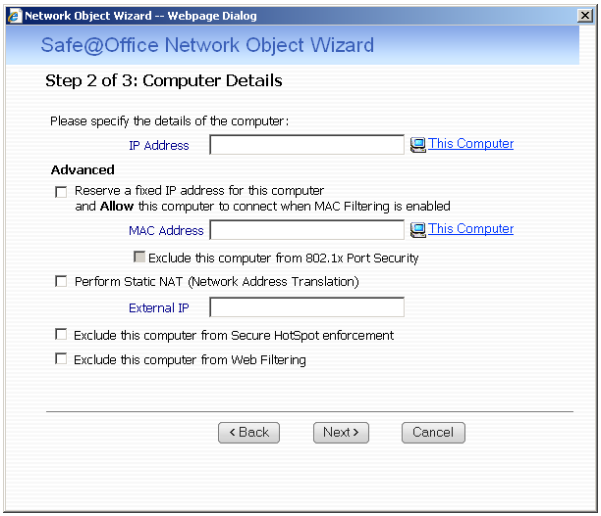
2. Do one of the following:
   - To add a network object, click **New**.
   - To edit an existing network object, click the Edit icon next to the desired computer in the list.

   The **Safe@Office Network Object Wizard** opens, with the **Step 1: Network Object Type** dialog box displayed.

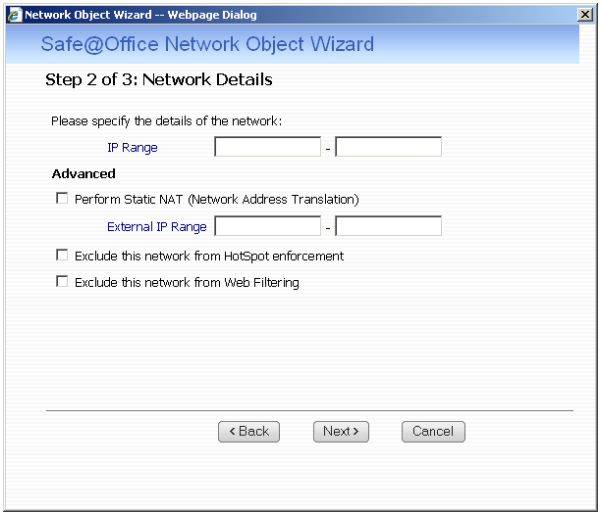

Network Object Wizard -- Webpage Dialog
Safe@Office Network Object Wizard
Step 1 of 3: Network Object Type
Which type of network object do you want to create?
Single Computer
Represents a single computer or network attached device on the internal network or on the Internet.
Network
Represents a range of consecutive IP addresses on the internal network or on the Internet.
Next >
Cancel

3. Do one of the following:
   - To specify that the network object should represent a single computer or device, click **Single Computer**.
   - To specify that the network object should represent a network, click **Network**.
4. Click **Next**.

The Step 2: Computer Details dialog box appears. If you chose Single Computer, the dialog box includes the Reserve a fixed IP address for this computer option.

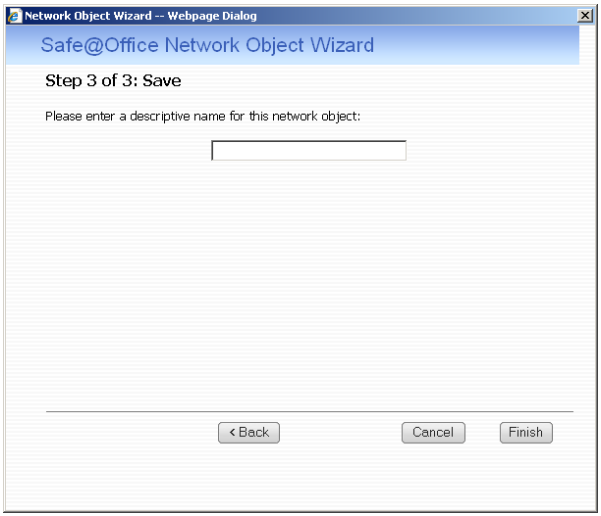

Network Object Wizard -- Webpage Dialog
Safe@Office Network Object Wizard
Step 2 of 3: Computer Details
Please specify the details of the computer:
IP Address
This Computer
Advanced
Reserve a fixed IP address for this computer
and Allow this computer to connect when MAC Filtering is enabled
MAC Address
This Computer
Exclude this computer from 802.1x Port Security
Perform Static NAT (Network Address Translation)
External IP
Exclude this computer from Secure HotSpot enforcement
Exclude this computer from Web Filtering
< Back
Next >
Cancel

If you chose Network, the dialog box does not include this option.


Network Object Wizard -- Webpage Dialog
Safe@Office Network Object Wizard
Step 2 of 3: Network Details
Please specify the details of the network:
IP Range
Advanced
Perform Static NAT (Network Address Translation)
External IP Range
Exclude this network from HotSpot enforcement
Exclude this network from Web Filtering
< Back
Next >
Cancel

5. Complete the fields using the information in the tables below.
6. Click Next.

The Step 3: Save dialog box appears.

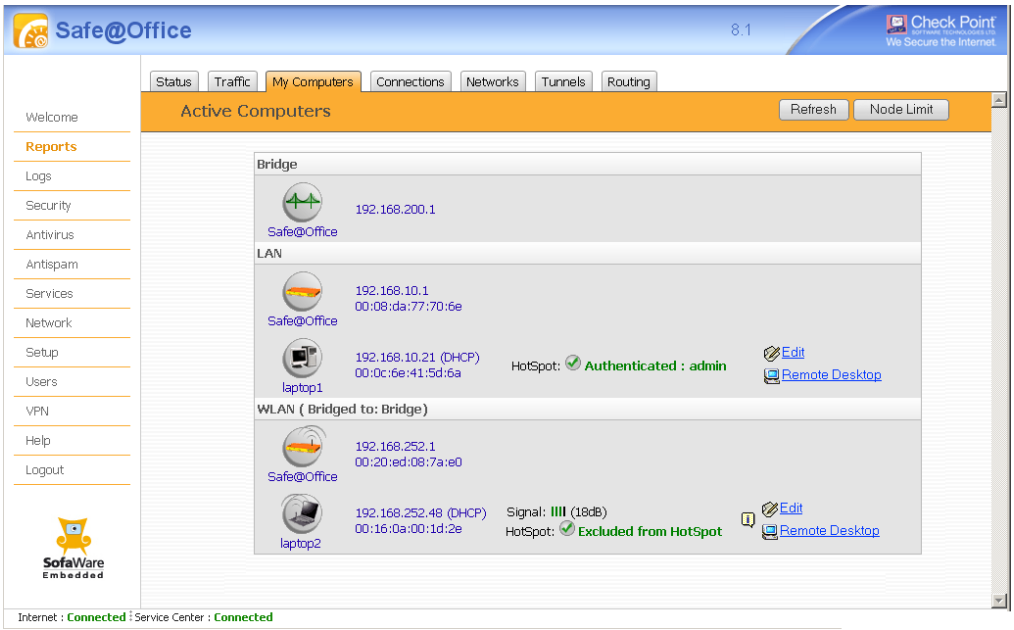

Network Object Wizard -- Webpage Dialog
Safe@Office Network Object Wizard
Step 3 of 3: Save
Please enter a descriptive name for this network object:
< Back
Cancel
Finish

7. Type a name for the network object in the field.
8. Click Finish.

To add or edit a network object via the My Computers page

1. Click Reports in the main menu, and click the My Computers tab.

The My Computers page appears.



If a computer has not yet been added as a network object, the Add button appears next to it. If a computer has already been added as a network object, the Edit button appears next to it.

2. Do one of the following:

   - To add a network object, click Add next to the desired computer.
   - To edit a network object, click Edit next to the desired computer.

   The Safe@Office Network Object Wizard opens, with the Step 1: Network Object Type dialog box displayed.

3. Do one of the following:

   - To specify that the network object should represent a single computer or device, click Single Computer.
   - To specify that the network object should represent a network, click Network.

4. Click Next.

   The Step 2: Computer Details dialog box appears.

The computer's IP address and MAC address are automatically filled in.

5. Complete the fields using the information in the tables below.
6. Click Next.

   The Step 3: Save dialog box appears with the network object's name. If you are adding a new network object, this name is the computer's name.
7. To change the network object name, type the desired name in the field.
8. Click Finish.

   The new object appears in the Network Objects page.

Table 39: Network Object Fields for a Single Computer

In this field…	Do this…
IP Address	Type the IP address of the local computer, or click This Computer to specify your computer.
Reserve a fixed IP address for this computer and Allow this computer to connect when MAC filtering is enabled	Select this option to assign the network object's IP address to a MAC address, and to allow the network object to connect to the WLAN when MAC Filtering is used. For information about MAC Filtering, see ***Configuring a Wireless Network*** on page 305. The MAC Address and Exclude this computer from 802.1x Port Security fields are enabled.
MAC Address	Type the MAC address you want to assign to the network object's IP address, or click This Computer to specify your computer's MAC address.

In this field...	Do this...
Exclude this computer from 802.1x Port Security	Select this option to exclude this computer from 802.1x port-based security enforcement. The computer will be able to connect to a Safe@Office appliance port and access the network without authenticating.
Perform Static NAT (Network Address Translation)	Select this option to map the local computer's IP address to an Internet IP address. You must then fill in the External IP field.
External IP	Type the Internet IP address to which you want to map the local computer's IP address.
Exclude this computer from HotSpot enforcement	Select this option to exclude this computer from Secure HotSpot enforcement. This computer will be able to access the network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access this computer without viewing the My HotSpot page.
Exclude this computer from Web Filtering	Select this option to exclude this computer from the Web Filtering service and Web rule enforcement.

Table 40: Network Object Fields for a Network

In this field…	Do this…
IP Range	Type the range of local computer IP addresses in the network.
Perform Static NAT (Network Address Translation)	Select this option to map the network's IP address range to a range of Internet IP addresses of the same size. You must then fill in the External IP Range field.
External IP Range	Type the Internet IP address range to which you want to map the network's IP address range.
Exclude this network from HotSpot enforcement	Select this option to exclude this network from Secure HotSpot enforcement. Computers on the excluded network will be able to access your network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access computers on the excluded network without viewing the My HotSpot page.
Exclude this network from Web Filtering	Select this option to exclude this network from the Web Filtering service and Web rules.

Viewing and Deleting Network Objects

500 1000N

To view or delete a network object

1. Click Network in the main menu, and click the Network Objects tab.

   The Network Objects page appears with a list of network objects.

2. To delete a network object, do the following:

   a. In the desired network object's row, click Erase.

      A confirmation message appears.

   b. Click OK.

      The network object is deleted.

Configuring Network Service Objects

500 1000N

You can add custom services as network service objects. This enables you to configure firewall rules, VStream Antivirus rules, custom NAT rules, and static routes for the services represented by the network service objects.

Defining network service objects can make your policies easier to understand and maintain. When a network service object is modified, the change automatically takes effect in all rules and settings that reference the network service object.

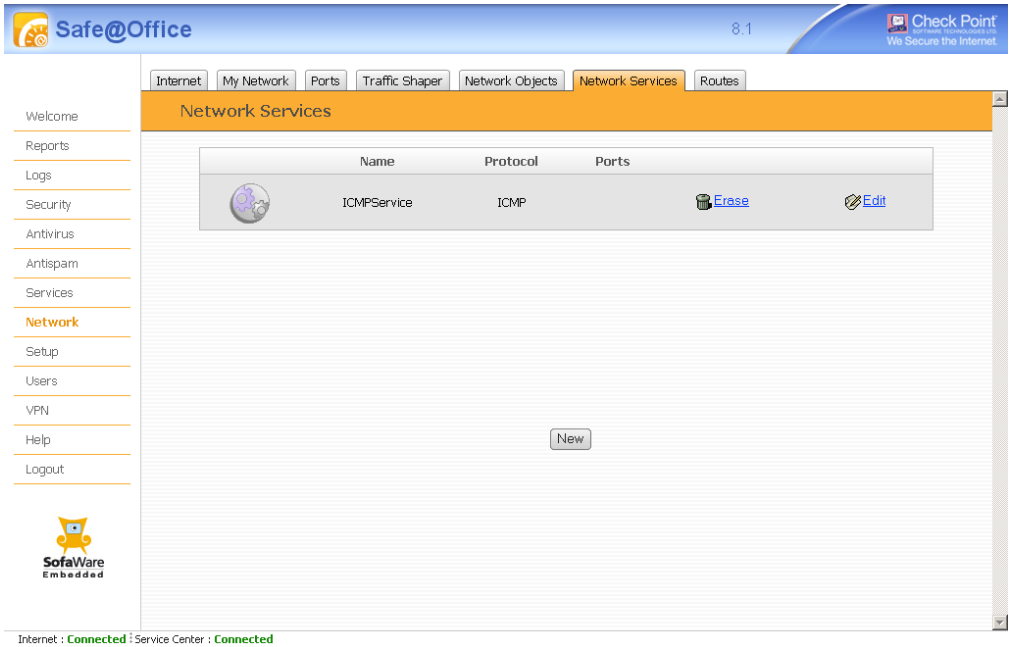
Adding and Editing Network Service Objects

500 1000N

To add or edit a network service object

1. Click Network in the main menu, and click the Network Services tab.

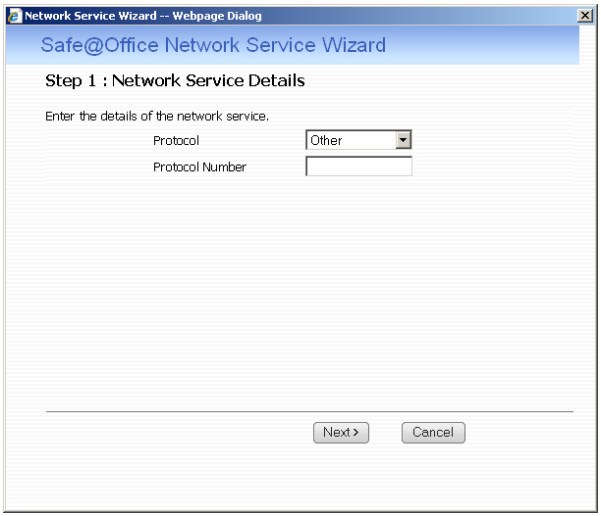
   The Network Services page appears with a list of network service objects.



2. Do one of the following:

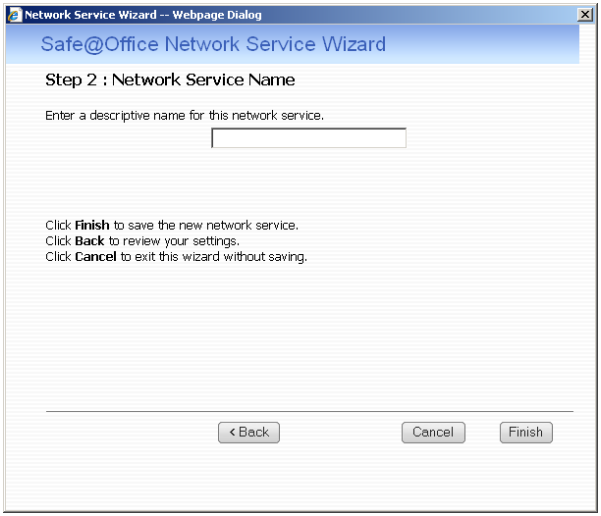
   - To add a network service object, click New.
   - To edit an existing network service object, click Edit next to the desired object in the list.

The Safe@Office Network Service Wizard opens, with the Step 1: Network Service Details dialog box displayed.



3. Complete the fields using the information in the table below.
4. Click Next.

   The Step 2: Network Service Name dialog box appears.


Network Service Wizard -- Webpage Dialog
Safe@Office Network Service Wizard
Step 2 : Network Service Name
Enter a descriptive name for this network service.
Click Finish to save the new network service.
Click Back to review your settings.
Click Cancel to exit this wizard without saving.
< Back
Cancel
Finish

5. Type a name for the network service object in the field.

6. Click Finish.

Table 41: Network Service Fields

In this field…	Do this…
Protocol	Select the network service's IP protocol. If you select Other, the Protocol Number field appears. If you select TCP or UDP, the Port Ranges field appears.
Protocol Number	Type the number of the network service's IP protocol.
Port Ranges	Type the network service's port or port ranges. Multiple ports or port ranges must be separated by commas. For example: "1000-1003,2000-2001,2005".

Viewing and Deleting Network Service Objects

500 1000N

To view or delete a network service object

1. Click Network in the main menu, and click the Network Services tab.
   The Network Services page appears with a list of network service objects.
2. To delete a network service object, do the following:
   a. In the desired network service object's row, click Erase.
      A confirmation message appears.
   b. Click OK.
      The network service object is deleted.

Using Static Routes

500 1000N

A static route is a setting that explicitly specifies the route to use for packets, according to *one* of the following criteria:

- The packet's source IP address and/or destination IP address
- The network service used to send the packet

Packets that match the criteria for a specific static route are sent to the route's defined destination, or *next hop*, which can be a specific gateway's IP address or an Internet connection. Specifying an Internet connection as the static route's next hop is useful in cases where the ISP's default gateway IP address is dynamically assigned to the gateway, as this approach allows you to route traffic to the Internet connection by specifying its name, instead of a static IP address.

Note: If the static route's next hop is an Internet connection that is currently unavailable, the Safe@Office appliance sends matching traffic through the static route with the next-lowest metric.

Packets with a source, destination, or network service that do not match any defined static route are routed to the default gateway. To modify the default gateway, see ***Using a LAN Connection*** on page 154.

When a static route is based on the packet's source, it is called a *source route*. Source routing can be used, for example, for load balancing between two Internet connections. For instance, if you have an Accounting department and a Marketing department, and you want each to use a different Internet connection for outgoing traffic, you can add a static route specifying that traffic originating from the Accounting department should be sent via WAN1, and another static route specifying that traffic originating from the Marketing department should be sent via WAN2.

A static route that is based on the network service used to send the packet is called a *service route*. Service routing is useful for directing all traffic of a particular type to a specific Internet connection. For example, you can choose to route all HTTP traffic to the secondary Internet connection, while routing all other traffic to the primary Internet connection. Service routes can be defined for network service objects, enabling you to create routes for custom protocols and port ranges.

The Static Routes page lists all existing routes, including the default, and indicates whether each route is currently "Up" (reachable) or not.

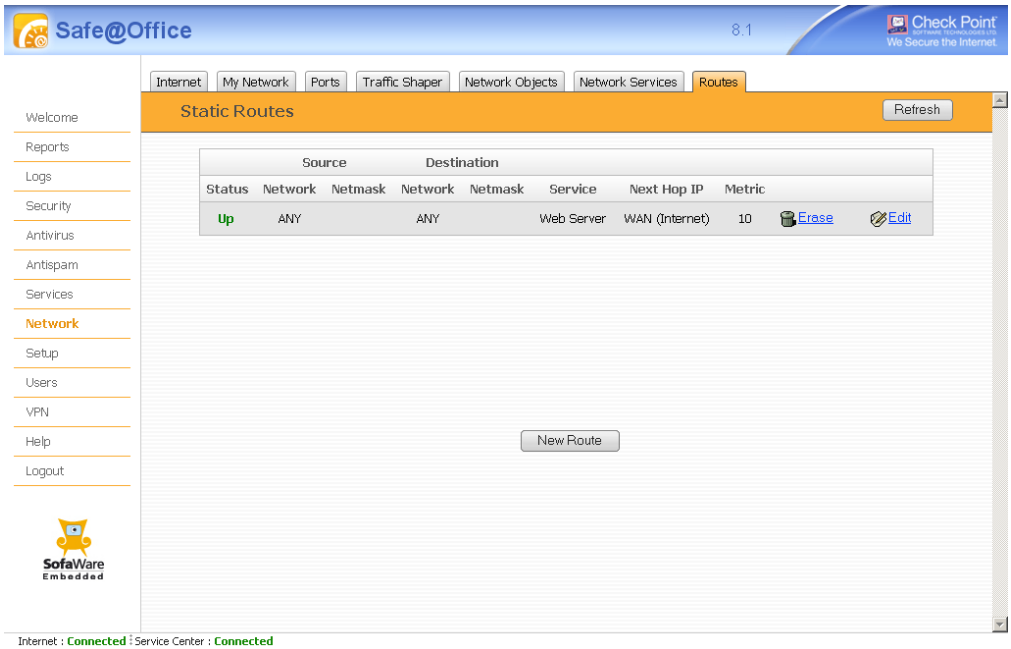
Adding and Editing Static Routes

500 1000N

To add a static route

1. Click Network in the main menu, and click the Routes tab.

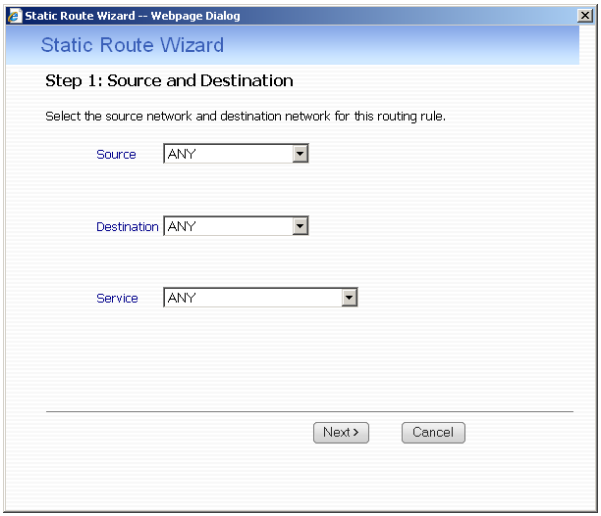
   The Static Routes page appears, with a list of existing static routes.



2. Do one of the following:

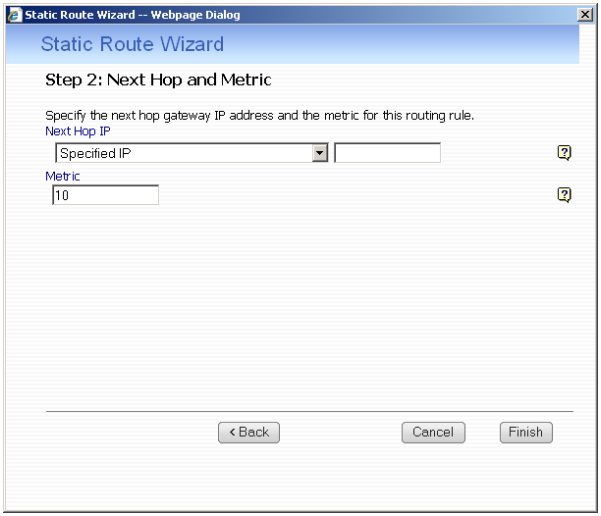
   - To add a static route, click New Route.
   - To edit an existing static route, click Edit next to the desired route in the list.

The Static Route Wizard opens displaying the Step 1: Source and Destination dialog box.



3. Complete the fields using the relevant information in the following table.
4. Click Next.

   The Step 2: Next Hop and Metric dialog box appears.



5. Complete the fields using the relevant information in the following table.

6. Click Next.

   The new static route is saved.

Table 42: Static Route Fields

In this field...	Do this...
Source	Specify the source network (source routing). This can be either of the following: • ANY. This route applies to packets originating in any network. • Specified Network. This route applies to packet originating in a specific network. The Network and Netmask fields appear.
Source - Network	Type the source network's IP address.
Source - Netmask	Select the source network's subnet mask.
Destination	Specify the destination network. This can be either of the following: • ANY. This route applies to packets sent to any network. • Specified Network. This route applies to packets sent to a specific network. The Network and Netmask fields appear.
Destination - Network	Type the destination network's IP address.
Destination - Netmask	Select the destination network's subnet mask.
Service	Specify the service used to send packets (service routing). This can be either of the following: • ANY. This route applies to packets sent using any service. • A specific service or network service object. Note: When defining a static route for a specific service, the Source and Destination fields must be set to ANY.

In this field...	Do this...
Next Hop IP	Specify the next hop to which packets should be sent. This can be any of the following: • Specified IP. Traffic matching this static route's criteria will be routed to a specific gateway. Type the IP address of the desired gateway (next hop router) in the field provided. • WAN (Internet). Traffic matching this static route's criteria will be routed to the Internet connection on the WAN1 interface. • WAN2 (Internet). Traffic matching this static route's criteria will be routed to the Internet connection on the WAN2 interface.
Metric	Type the static route's metric. When a packet matches multiple static routes' criteria, the gateway sends the packet to the matching route with the lowest metric. The default value is 10.

Viewing and Deleting Static Routes

500 1000N

To view or delete a static route

1. Click Network in the main menu, and click the Routes tab.
   The Static Routes page appears, with a list of existing static routes.
2. To refresh the view, click Refresh.
3. To delete a route, do the following:
   a. In the desired route's row, click Erase.
      A confirmation message appears.
   b. Click OK.
      The route is deleted.

Managing Ports

500 1000N

The Safe@Office appliance enables you to quickly and easily assign its ports to different uses, as shown in the following table. If desired, you can also disable ports.

Table 43: Ports and Assignments

You can assign this port...	To these uses...
LAN 1-4	LAN network
	A WAN Internet connection
	A port-based VLAN
	A VLAN that is dynamically assigned by a RADIUS server, as part of an 802.1x port-based security scheme
DMZ/WAN2	DMZ network
	A WAN Internet connection
	VLAN trunk
	A port-based VLAN
	A VLAN that is dynamically assigned by a RADIUS server, as part of an 802.1x port-based security scheme
DSL	An ADSL Internet connection
WAN	A WAN Internet connection
Serial	RS232 modem
	Serial console
ExC	An ExpressCard cellular modem

You can assign this port...	To these uses...
USB	Printers
	USB-based modems

The Safe@Office appliance also allows you to restrict each port to a specific link speed and duplex setting and to configure its security scheme. For information on port-based security, see ***Using Port-Based Security*** on page 413.

Viewing Port Statuses

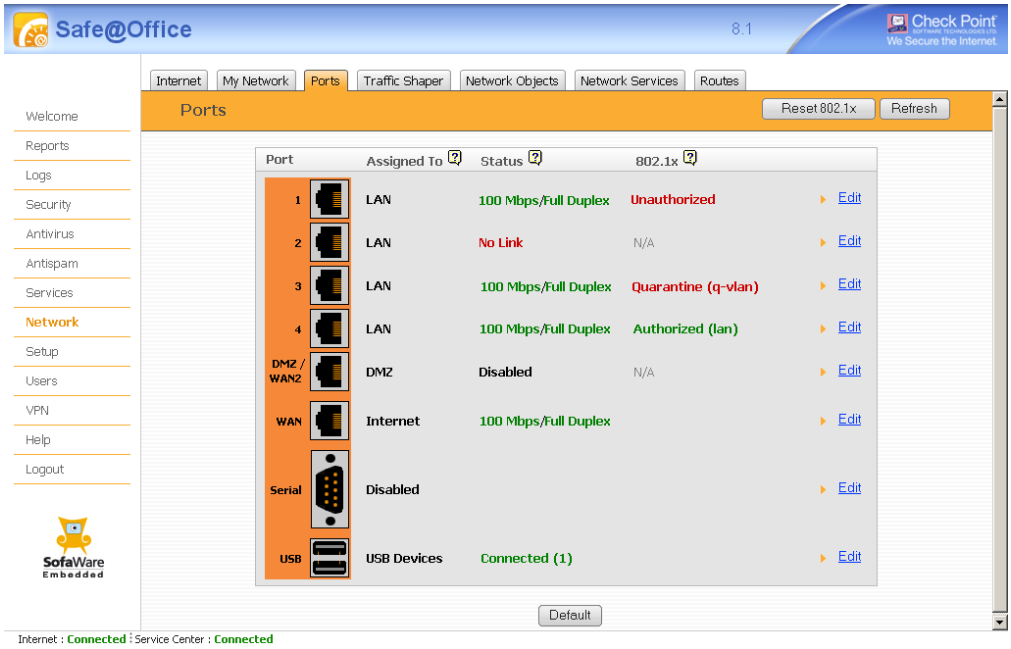
500 1000N

You can view the status of the Safe@Office appliance's ports on the Ports page, including each Ethernet connection's duplex state. This is useful if you need to check whether the appliance's physical connections are working, and you can’t see the LEDs on front of the appliance.

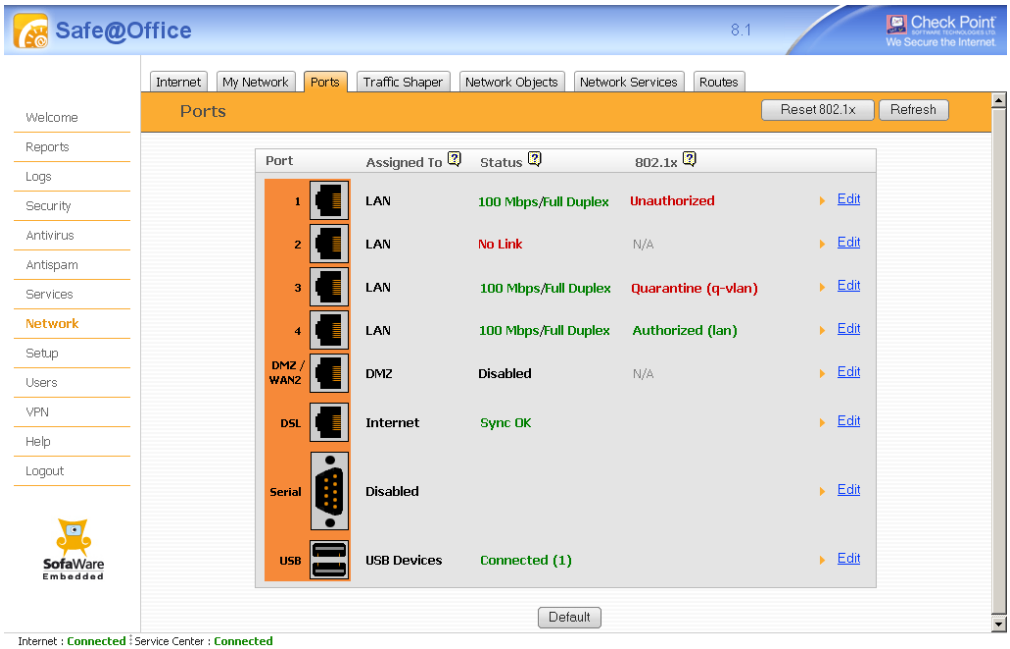
To view port statuses

1. Click Network in the main menu, and click the Ports tab.

The Ports page appears. In non-ADSL models, this page appears as follows:



In ADSL models, this page appears as follows:



The page displays the information for each port, as described in the following table.

2. To refresh the display, click Refresh.

Table 44: Ports Fields

This field...	Displays...
Assign To	The port's current assignment. For example, if the DMZ/WAN2 port is currently used for the DMZ, the field displays "DMZ".

This field...	Displays...
Status	The port's current status. Ethernet ports can have the following statuses:

Status	Description
The detected link speed and duplex (Full Duplex or Half Duplex)	The port is in use.
No Link	The appliance does not detect anything connected to the port.
Disabled	The port is disabled. For example, the DMZ/WAN2 port's status will be "Disabled" if the port is assigned to "None", or if it assigned to "DMZ" and the DMZ is disabled.

This field...	Displays...

The ADSL port can have the following statuses:

Status	Description
Sync OK	The ADSL modem synchronized with the ADSL service provider.
No Sync	The ADSL modem failed to synchronize with the ADSL service provider. Check that a micro-filter is properly connected, and check that your DSL Standard setting is compatible with your service provider. You can view this setting in the Network > Internet Setup page.
Disabled	The port is disabled. The port's status will be disabled, if it is assigned to "None".

This field...	Displays...

The USB port can have the following statuses:

Status	Description
Connected (number)	USB devices (printers or modem) are connected to the USB ports. The number of connected devices appears in parentheses.
Not Connected	No USB devices are connected to the USB ports.

The ExC port can have the following statuses:

Status	Description
Connected (number)	A ExpressCard modems is inserted in the ExpressCard slot.
Not Connected	No ExpressCard modem is inserted in the ExpressCard slot.

<table>
<tr><th>This field…</th><th>Displays…</th></tr>
<tr><td>802.1x</td><td>The port's security scheme. This can be any of the following:
<table>
<tr><th>Scheme</th><th>Description</th></tr>
<tr><td>N/A</td><td>No security scheme is defined for the port.</td></tr>
<tr><td>Unauthorized</td><td>An 802.1x security scheme is defined for the port. Users have not yet connected to the port and attempted to authenticate, or a user failed to authenticate and no Quarantine network is configured.</td></tr>
<tr><td>Authorized (network)</td><td>An 802.1x security scheme is defined for the port. A user connected to the port, authenticated successfully, and was assigned to a network. The name of the assigned network appears in parentheses.</td></tr>
<tr><td>Quarantine (network)</td><td>An 802.1x security scheme is defined for the port. A user connected to the port, failed to authenticate, and was assigned to the Quarantine network. The name of the Quarantine network appears in parentheses.</td></tr>
</table>
For information on configuring 802.1x port-based security, see Using Port-Based Security on page 413.</td></tr>
</table>

Modifying Port Assignments

500 1000N

You can assign ports to different networks or purposes. Since modifying port assignments often requires additional configurations, use the following table to determine which procedure you should use.

Table 45: Modifying Port Assignments

To assign a port to...	See...
No network	The procedure below. This disables the port.
LAN	The procedure below
VLAN or VLAN Trunk	***Configuring VLANs*** on page 216
A WAN Internet connection	The procedure below. Note: When you configure an Ethernet-based Internet connection on a port, the port is automatically assigned to Internet use. For information on configuring an Internet connection, see ***Using Internet Setup*** on page 141.
DMZ	Configuring a DMZ Network
Console	***Using a Console*** on page 714
A VLAN network, dynamically assigned by a RADIUS server	***Configuring Port-Based Security*** on page 415
A printer	***Setting Up Network Printers*** on page 768
An RS232 Modem	***Setting Up an RS232 Modem*** on page 177
A USB-based modem	***Setting Up a USB Modem*** on page 181

To assign a port to...	See...
An ExpressCard modem	***Setting Up an ExpressCard Cellular Modem*** on page 185

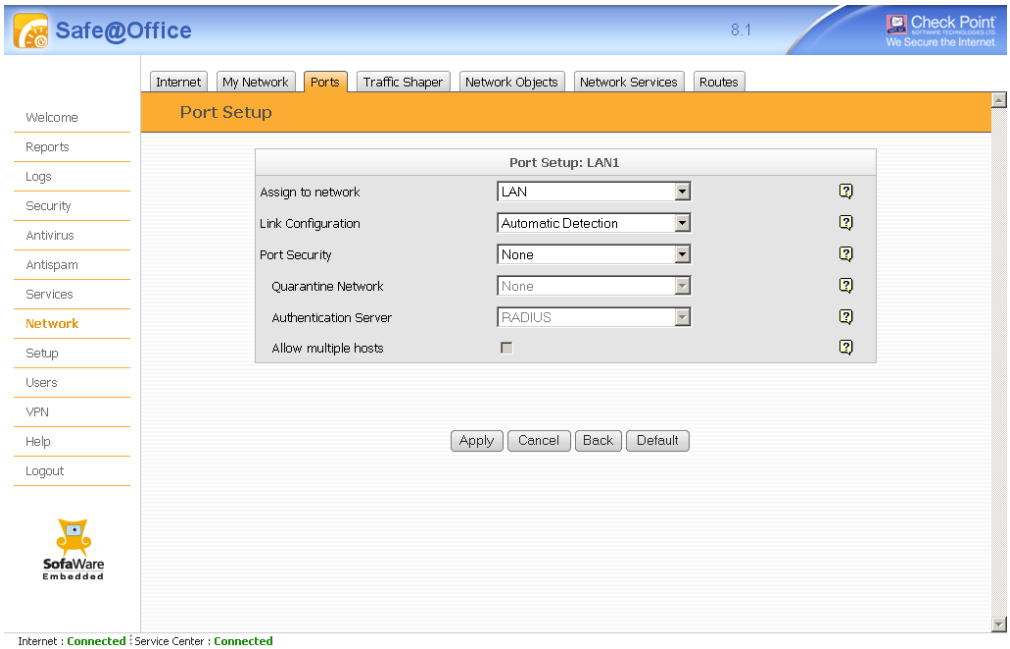
To modify a port assignment

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.



3. In the Assign to Network drop-down list, do one of the following:

   - To assign a network port to the LAN, select LAN.
   - To configure a network port for use with a WAN Internet connection, select Internet.
   - To disable a network port, select None.

- To disable the Serial port, select Disabled.

4. Click Apply.

   A warning message appears.

5. Click OK.

   The port is reassigned to the specified network or purpose.

Modifying Link Configurations

500 1000N

By default, the Safe@Office appliance automatically detects the link speed and duplex. If desired, you can manually restrict the appliance's ports to a specific link speed and duplex setting.

To modify a port's link configuration

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.

3. In the Link Configuration drop-down list, do one of the following:

   - Select the desired link speed and duplex.
   - Select Automatic Detection to configure the port to automatically detect the link speed and duplex.

     This is the default.

4. Click Apply.

   A warning message appears.

5. Click OK.

   The port uses the specified link speed and duplex.

Resetting Ports to Defaults

500 1000N

You can reset the Safe@Office appliance's ports to their default link configurations ("Automatic Detection") and default assignments (shown in the following table).

Table 46: Default Port Assignments

Port	Default Assignment
LAN 1-4	LAN
DMZ / WAN2	DMZ
WAN	This port is always assigned to the WAN.
ADSL	This port is always assigned to the WAN.
Serial	Console

Note: Resetting ports to their defaults may result in the loss of your Internet connection. Therefore, it is recommended to be particularly careful when performing this procedure remotely.

Resetting All Ports to Defaults

500 1000N

To reset all ports to defaults

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Click Default.

   A confirmation message appears.

3. Click OK.

   All ports are reset to their default assignments and to "Automatic Detection" link configuration.

Resetting Individual Ports to Defaults

500 1000N

To reset a port to defaults

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.

3. Click Default.

   A confirmation message appears.

4. Click OK.

   The port is reset to its default assignment and to "Automatic Detection" link configuration.

Chapter 7

Using Bridges

This chapter describes how to connect multiple network segments at the data-link layer, using a bridge.

This chapter includes the following topics:

Overview 259
Workflow....265
Adding and Editing Bridges 266
Adding Internal Networks to Bridges....270
Adding Internet Connections to Bridges 274
Deleting Bridges....278

Overview

The Safe@Office appliance enables you to connect multiple network segments at the data-link layer, by configuring a bridge. Bridges offer the following advantages:

- Easy network segmentation

  Bridges can be used to compartmentalize an existing network into several security zones, without changing the IP addressing scheme or the routers' configuration.

  Ordinarily, if you need to deploy a firewall within an internal network, you can divide the existing subnet into two networks and configure a new routing scheme. However, in some deployments, the amount of network reconfiguration required prohibits such a solution. Adding a bridge not only allows you to segment your network quickly and easily, but it allows you to choose whether to enable the firewall between network segments.

If you enable the firewall between bridged network segments, the gateway operates as a regular firewall between network segments, inspecting traffic and dropping or blocking unauthorized or unsafe traffic. In contrast, if you disable the firewall between bridged network segments, all network interfaces assigned to the bridge are connected directly, with no firewall filtering the traffic between them. The network interfaces operate as if they were connected by a hub or switch.

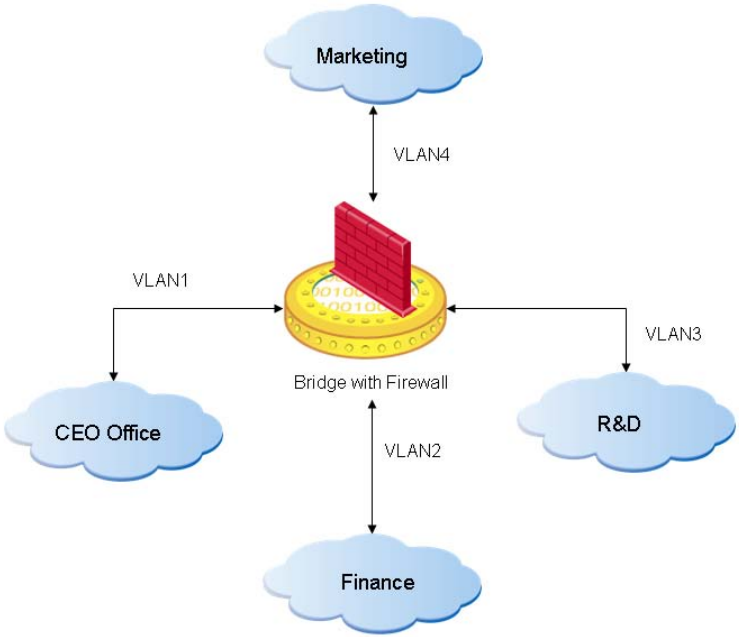


Figure 29: Bridge with Four VLANs

For example, if you assign the LAN and primary WLAN networks to a bridge and disable the bridge's internal firewall, the two networks will act as a single, seamless network, and only traffic from the LAN and primary WLAN networks to other networks (for example, the Internet) will be inspected by the firewall. If you enable the internal firewall, it will enforce security rules and inspect traffic between the LAN and primary WLAN networks.

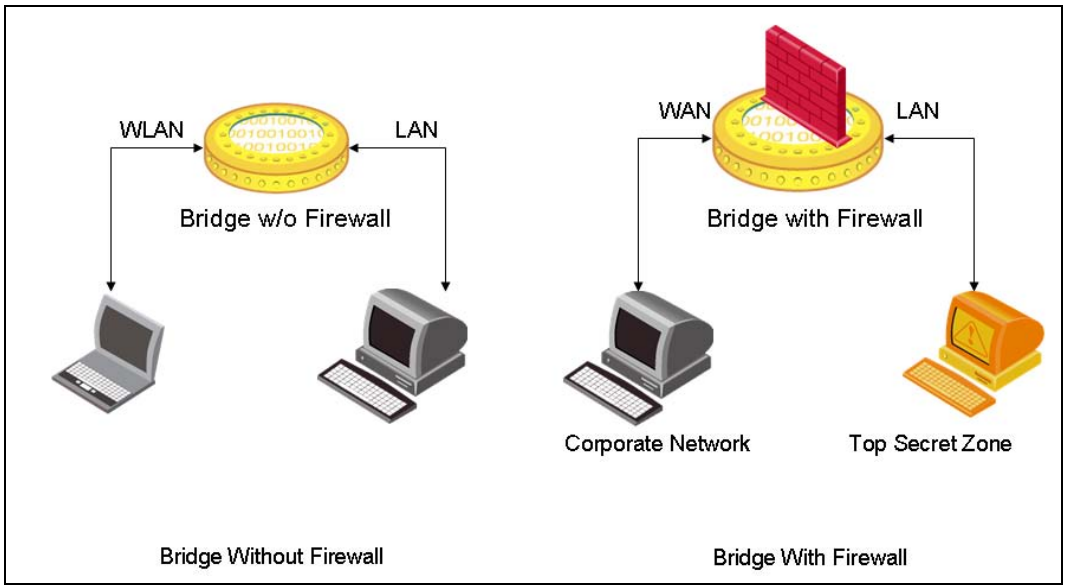


Figure 30: Bridge Firewalling

- Transparent roaming

  In a routed network, if a host is physically moved from one network area to another, then the host must be configured with a new IP address. However, in a bridged network, there is no need to reconfigure the host, and work can continue with minimal interruption.

The Safe@Office appliance allows you to configure anti-spoofing for bridged network segments. When anti-spoofing is configured for a segment, only IP addresses within a specific IP address range can be sent from that network segment. For example, if you configure anti-spoofing for the "Marketing" network segment, the following things happens:

- If a host with an IP address *outside of the allowed IP address range* tries to connect from a port or VLAN that belongs to the "Marketing" network segment, the connection will be blocked and logged as "Spoofed IP".
- If a host with an IP address within the bridge IP address range tries to connect from a port or VLAN that belongs to a network segment *other than the "Marketing" segment*, the connection will be blocked and logged as "Spoofed IP".

Note: The following Safe@Office models do not support using bridge mode with port-based VLAN:

- SBX166-LHGE-2
- SBX166-LHGE-3

Note: If the Safe@Office 1000N Power Pack upgrade is not installed, you can configure only one bridge.

How Does Bridge Mode Work?

Bridges operate at layer 2 of the OSI model, therefore adding a bridge to an existing network is completely transparent and does not require any changes to the network's structure.

Each bridge maintains a forwarding table, which consists of `<MAC Address, Port>` associations. When a packet is received on one of the bridge ports, the forwarding table is automatically updated to map the source MAC address to the network port from which the packet originated, and the gateway processes the received packet according to the packet's type.

When a bridge receives an IP packet, the gateway processes the packet as follows:

1. The destination MAC address is looked up in the bridge's forwarding table.
2. If the destination MAC address is found in the forwarding table, the packet is forwarded to the corresponding port.
3. If the destination MAC address is not found in the forwarding table, the destination IP address is searched for in all the defined bridge IP address ranges.
4. If the destination IP address is found in the bridge IP address range of exactly one port, the IP address is transmitted to that port.
5. If the IP address is found in the bridge IP address range of more than one port, the packet is dropped. The gateway then sends an ARP query to each of the relevant ports.
6. If a host responds to the ARP request packet with an ARP reply, the forwarding table is updated with the correct `<MAC Address, Port>` association. Subsequent packets will be forwarded using the forwarding table.

If a bridge receives a non-IP packet, and the bridge is configured to forward non-IP protocol Layer-2 traffic, the gateway processes the packet as follows:

1. The destination MAC address is looked up in the bridge's forwarding table.
2. If the destination MAC address is found in the forwarding table, the packet is forwarded to the corresponding port.
3. If the destination MAC address is not found in the forwarding table, the packet is flooded to all the ports on the bridge.

Multiple Bridges and Spanning Tree Protocol

When using multiple bridges, you can enable fault tolerance and optimal packet routing, by configuring Spanning Tree Protocol (STP - IEEE 802.1d). When STP is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.

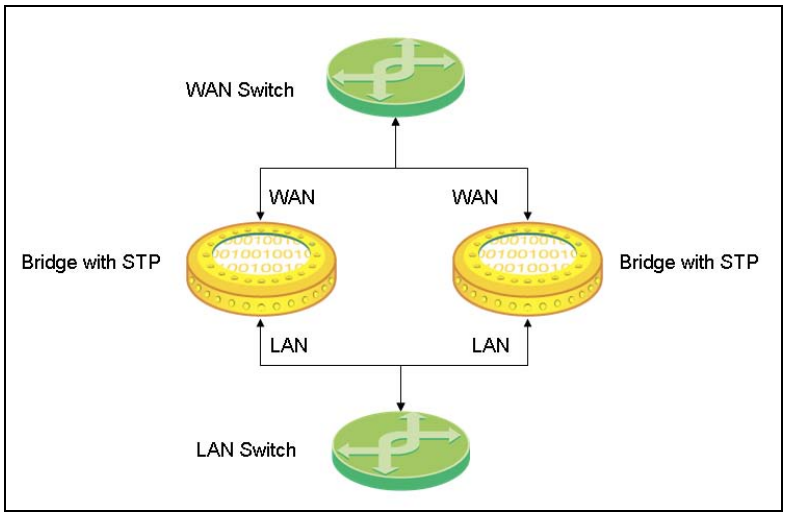


Figure 31: Dual Redundant Bridges with STP

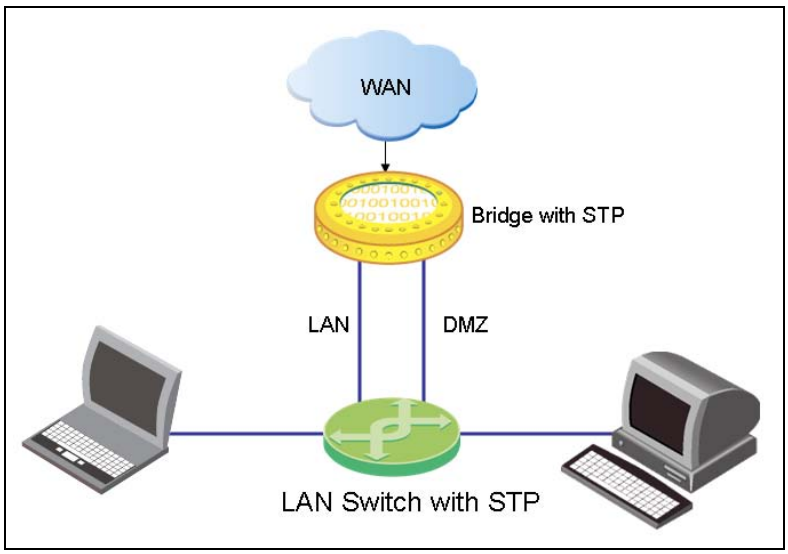


Figure 32: Link Redundancy with STP

Workflow

500 1000N

To use a bridge

1. Add a bridge.

   See ***Adding and Editing Bridges*** on page 266.

2. Add the desired internal networks to the bridge.

   See ***Adding Internal Networks to Bridges*** on page 270.

3. Add the desired Internet connections to the bridge.

   See ***Adding Internet Connections to Bridges*** on page 274.

4. If you enabled the firewall between networks on this bridge, add security rules and VStream Antivirus rules as needed.

For information on adding security rules, see ***Adding and Editing Rules*** on page 404. For information on adding VStream Antivirus rules, see ***Adding and Editing Vstream Antivirus Rules*** on page 512.

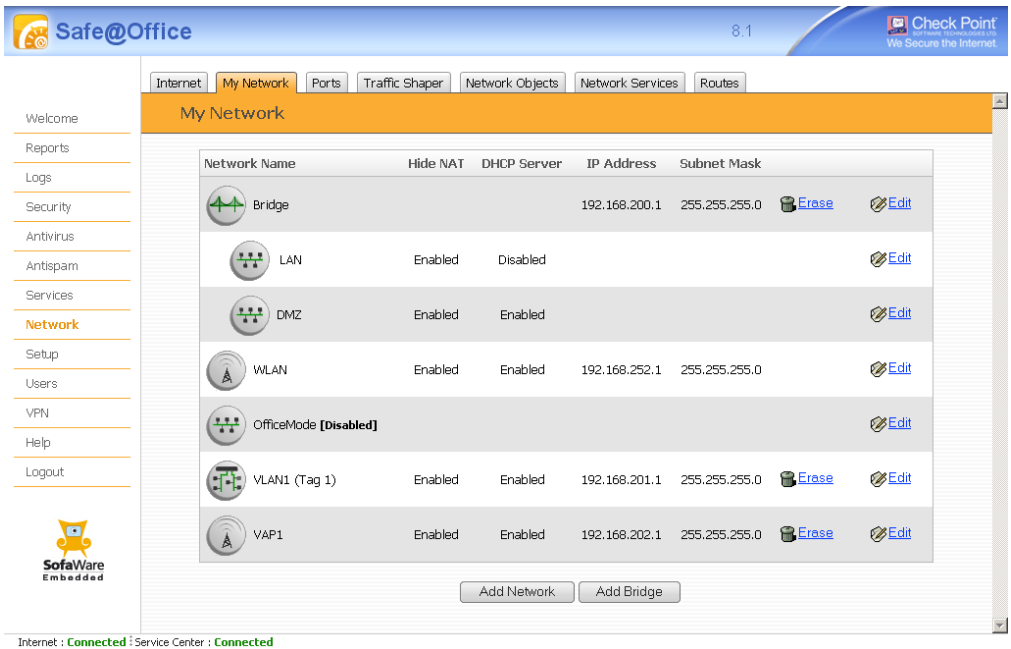
Adding and Editing Bridges

500 1000N

To add or edit a bridge

1. Click Network in the main menu, and click the My Network tab.

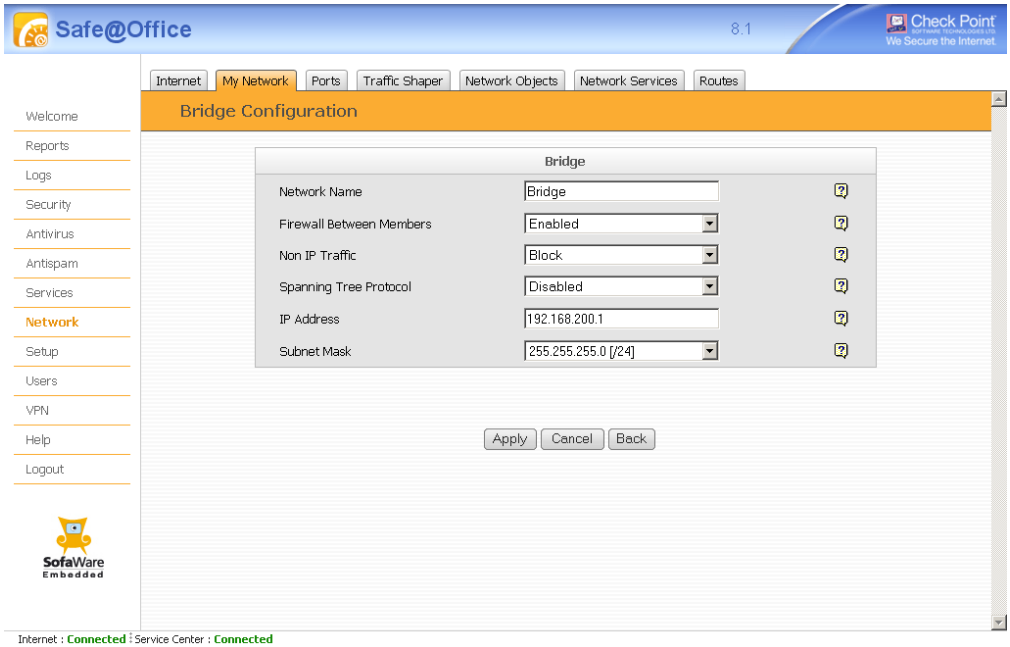
   The My Network page appears.



2. Do one of the following:

   - To add a bridge, click Add Bridge.
   - To edit a bridge, click Edit in the desired bridge's row.

The **Bridge Configuration** page appears.



3. Complete the fields using the following table.
4. Click **Apply**.

   A success message appears.

Table 47: Bridge Configuration Fields

In this field…	Do this…
Network Name	Type a name for the bridge.
Firewall Between Members	Specify whether the firewall should be enabled between networks on this bridge, by selecting one of the following: • Enabled. The firewall is enabled, and it will inspect traffic between networks on the bridge, enforcing firewall rules and SmartDefense protections. This is the default value. • Disabled. The firewall is disabled between networks on the bridge.
Non IP Traffic	Specify how the firewall should handle non-IP protocol traffic between networks on this bridge, by selecting one of the following: • Block. The firewall will block all non-IP protocol traffic on the bridge. This is the default value. • Pass. The firewall will allow all non-IP protocol traffic on the bridge and process it as described in ***Using Bridges*** on page 259.
Spanning Tree Protocol	Specify whether to enable STP for this bridge, by selecting one of the following: • Enabled. STP is enabled. • Disabled. STP is disabled. This is the default value. If you selected Enabled, the Bridge Priority field appears.

In this field...	Do this...
Bridge Priority	Select this bridge's priority. The bridge's priority is combined with a bridged network's MAC address to create the bridge's ID. The bridge with the lowest ID is elected as the root bridge. The other bridges in the tree calculate the shortest distance to the root bridge, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this bridge being elected as the root bridge, select a lower priority. Note: If you select the same priority for all bridges, the root bridge will be elected based on MAC address. The default value is 32768. This field only appears if STP is enabled.
IP Address	Type the IP address to use for this gateway on this bridge. Note: The bridge must not overlap other networks.
Subnet Mask	Select this bridge's subnet mask.

Adding Internal Networks to Bridges

500 1000N

Note: In order to add a VLAN of any type (port-based, tag-based, VAP, or WDS link) to the bridge, you must first create the desired VLAN.

For information on adding port-based VLANs, see ***Adding and Editing Port-Based VLANs*** on page 220. For information on adding tag-based VLANs, see ***Adding and Editing Tag-Based VLANs*** on page 222.For information on adding VAPs, see ***Configuring Virtual Access Points*** on page 333. For information on adding WDS links, see ***Configuring WDS Links*** on page 338.

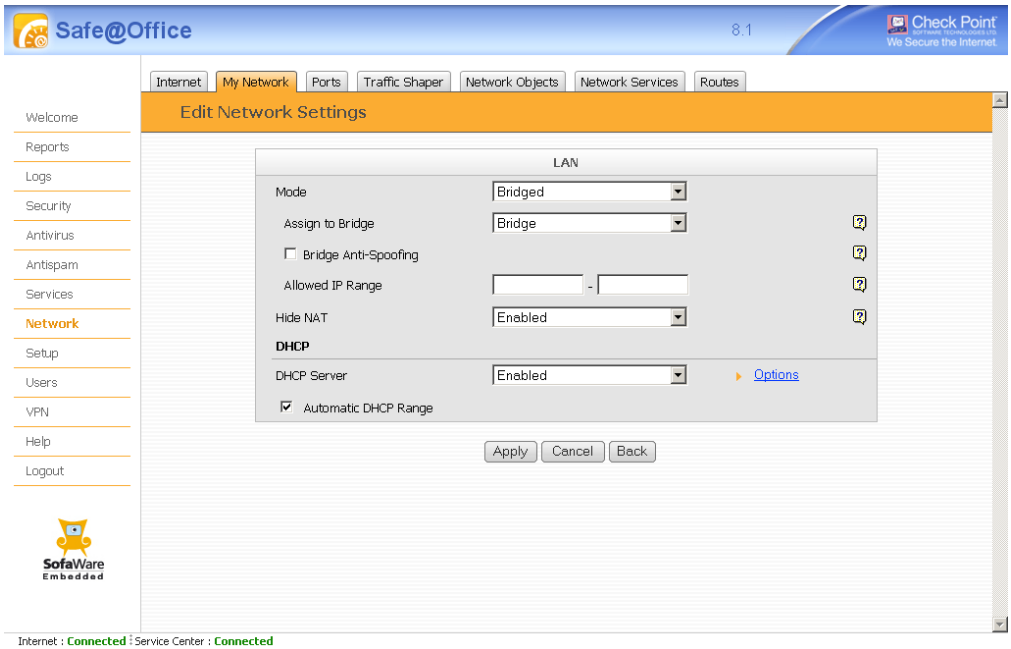
To add an internal network to a bridge

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

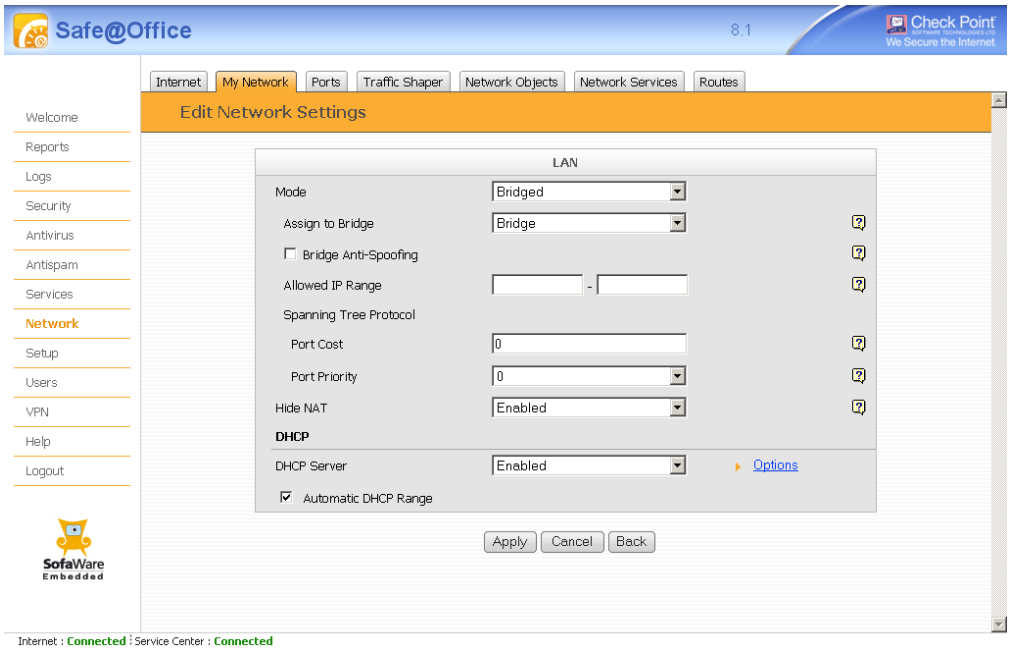
2. Click Edit in the desired network's row.
3. In the Mode drop-down list, select Bridged.

New fields appear.



4. Complete these fields as described below.

If the assigned bridge uses STP, additional fields appear.



5. Click Apply.

   A warning message appears.

6. Click OK.

   A success message appears.

   In the My Network page, the internal network appears indented under the bridge.

Table 48: Bridged Network Fields

In this field…	Do this…
Assign to Bridge	Select the bridge to which the network should be assigned.
Bridge Anti-Spoofing	Select this option to enable anti-spoofing. If anti-spoofing is enabled, only IP addresses within the Allowed IP Range can be source IP addresses for packets on this network.
Allowed IP Range	Type the range of IP addresses that should be allowed on this network. Note: When assigning IP addresses to machines in a bridged network segment, the Safe@Office DHCP server allocates only addresses within the allowed IP address range. To enable clients to move between bridged networks without changing IP addresses, configure identical IP address ranges for the desired networks, thus allowing the IP addresses to be used on either of the bridged networks. Note: Configuring overlapping or identical allowed IP address ranges will decrease the effectiveness of anti-spoofing between the bridged networks.
Spanning Tree Protocol - Port Cost	Type the port's cost. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. This field only appears if the bridge uses STP.

In this field...	Do this...
Spanning Tree Protocol - Port Priority	Select the port's priority. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. The default value is 128. This field only appears if the bridge uses STP.

Adding Internet Connections to Bridges

500 1000N

To add an Internet connection to a bridge

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

2. Next to the desired Internet connection, click Edit.

   The Internet Setup page appears.

3. In the Port drop-down list, specify the port that the Internet connection should use, by doing one of the following:

   - To use the ADSL port, select ADSL.

This option is available in ADSL models only.

- To use the WAN port, select WAN.

  This option is available in non-ADSL models only.

- To use the DMZ/WAN2 port, select WAN2.

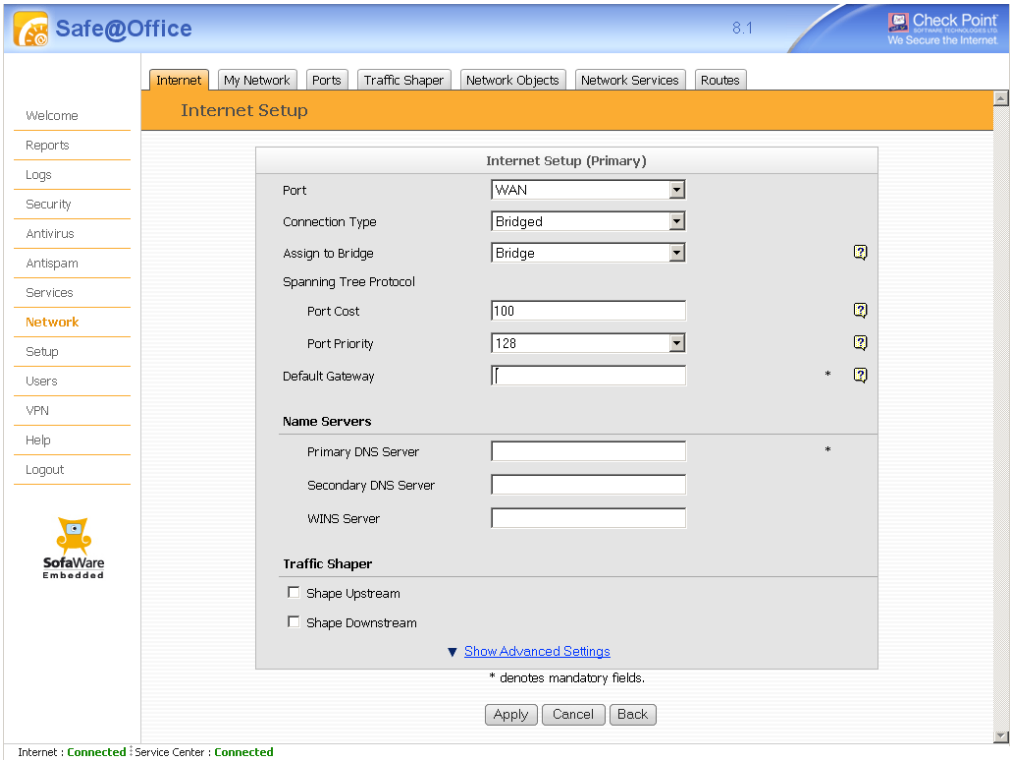
4. Do one of the following:

   - To configure a Bridged PPPoA connection, in the Connection Type field, select PPPoA.

     This option is available in ADSL models only.

   - Otherwise, in the Connection Type field, select Bridged.

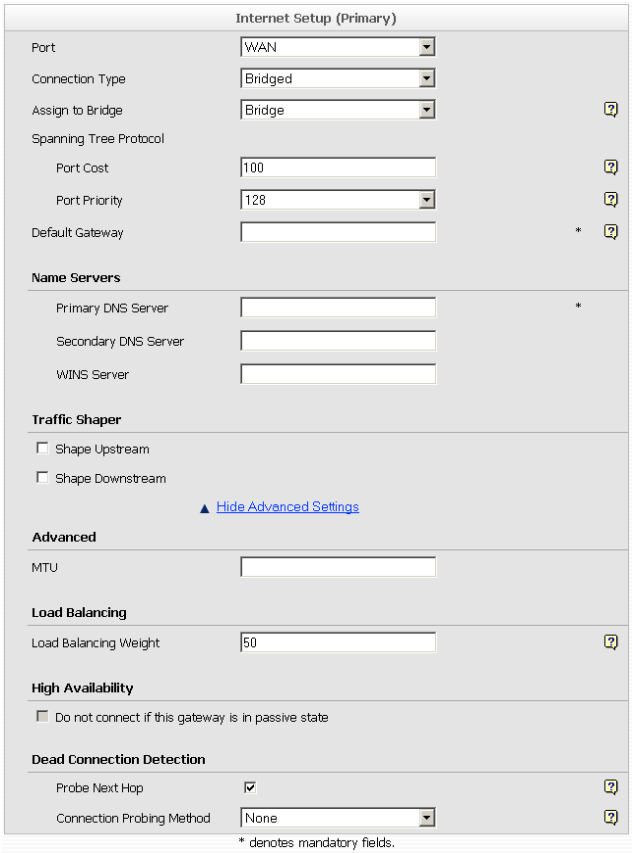
   New fields appear.



5. Complete the fields specified in the table below.

6. Complete the rest of the fields using the relevant information in ***Internet Setup Fields*** on page 168.

   New fields appear, depending on the selected options, and whether the selected bridge uses STP.



7. Click Apply.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Table 49: Bridged Connection Fields

In this field…	Do this…
Bridge Mode	Select this option to configure a Bridged PPPoA connection. The Bridge To field appears. This field is relevant for Bridged PPPoA connections only.
Bridge To	Select the bridge to which you want to add the PPPoA connection. This field is relevant for Bridged PPPoA connections only.
Assign to Bridge	Select the bridge to which the connection should be assigned. This field is relevant for regular bridged connections only.
Spanning Tree Protocol - Port Cost	Type the port's cost. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. This field only appears if the selected bridge uses STP. It is relevant for regular bridged connections only.

In this field...	Do this...
Spanning Tree Protocol - Port Priority	Select the port's priority. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. The default value is 128. This field only appears if the selected bridge uses STP. It is relevant for regular bridged connections only.

Deleting Bridges

500 1000N

To delete a bridge

1. Remove all internal networks from the bridge, by doing the following for each network:
   a. Click Network in the main menu, and click the My Network tab.
      The My Network page appears.
   b. Click Edit in the desired network's row.
   c. In the Mode drop-down list, select Enabled.
   d. Click Apply.

2. Remove all Internet connections from the bridge, by doing the following for each connection:
   a. Click Network in the main menu, and click the Internet tab.

      The Internet page appears.
   b. Next to the desired Internet connection, click Edit.
   c. The Internet Setup page appears.
   d. In the Connection Type field, select the desired connection type (not Bridged).
   e. Click Apply.
3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
4. In the desired bridge's row, click Erase.

   A confirmation message appears.
5. Click OK.

   The bridge is deleted.

Chapter 8

Configuring High Availability

This chapter describes how to configure High Availability (HA) for two or more Safe@Office appliances.

This chapter includes the following topics:

Overview 281
Configuring High Availability on a Gateway 284
Sample Implementation on Two Gateways 289

Overview

You can create a High Availability (HA) cluster consisting of two or more Safe@Office appliances. For example, you can install two Safe@Office appliances on your network, one acting as the “Master”, the default gateway through which all network traffic is routed, and one acting as the “Backup”. If the Master fails, the Backup automatically and transparently takes over all the roles of the Master. This ensures that your network is consistently protected by a Safe@Office appliance and connected to the Internet.

The gateways in a HA cluster each have a separate IP address within the local network. In addition, the gateways share a single virtual IP address, which is the default gateway address for the local network. Control of the virtual IP address is passed as follows:

1. Each gateway is assigned a priority, which determines the gateway's role: the gateway with the highest priority is the "Active Gateway" and uses the virtual IP address, and the rest of the gateways are "Passive Gateways".
2. The Active Gateway sends periodic signals, or “heartbeats”, to the network via a synchronization interface.

   The synchronization interface can be any internal network or bridge existing on both gateways, except the WAN interface and the primary WLAN.
3. If the heartbeat from the Active Gateway stops (indicating that the Active Gateway has failed), the gateway with the highest priority becomes the new Active Gateway and takes over the virtual IP address.

4. When a gateway that was offline comes back online, or a gateway's priority changes, the gateway sends a heartbeat notifying the other gateways in the cluster.

   If the gateway's priority is now the highest, it becomes the Active Gateway.

The Safe@Office appliance supports Internet connection tracking, which means that each appliance tracks its Internet connection's status and reduces its own priority by a user-specified amount, if its Internet connection goes down. If the Active Gateway's priority drops below another gateway's priority, then the other gateway becomes the Active Gateway.

Note: You can force a fail-over to a passive Safe@Office appliance. You may want to do this in order to verify that HA is working properly, or if the active Safe@Office appliance needs repairs. To force a fail-over, switch off the primary box or disconnect it from the LAN network.

The Safe@Office appliance supports configuring multiple HA clusters on the same network segment. To this end, each cluster must be assigned a unique ID number.

When HA is configured, you can specify that only the Active Gateway in the cluster should connect to the Internet. This is called WAN HA, and it is useful in the following situations:

- Your Internet subscription cost is based is on connection time, and therefore having the Passive appliances needlessly connected to the Internet costs you money.
- You want multiple appliances to share the same static IP address without creating an IP address conflict.

WAN HA avoids an IP address change, and thereby ensures virtually uninterrupted access from the Internet to internal servers at your network.

On the other hand, you might prefer to keep Passive Gateways connected to the Internet at all times, so that they can download updates from the Service Center and be accessible for remote management, even when not acting as the Active Gateway. In this case, you must assign a virtual IP address to the WAN interface. Each Passive Gateway will remain constantly connected to the Internet using its WAN interface's primary IP address, while remaining on standby to take over the WAN virtual IP address, in the event that the Active Gateway fails. If desired, you can configure a WAN virtual IP address for the WAN2 interface, as well.

Note: To use a WAN virtual IP address, the Internet connection method must be "Static IP". PPP-based connections and dynamic IP connections are not supported.

Before configuring HA, the following requirements must be met:

- You must have at least two identical Safe@Office appliances.
- The appliances must have identical firmware versions and firewall rules.
- The appliances' internal networks and bridges must be the same.
- The appliances must have *different* real internal IP addresses, but share *the same* virtual IP address.
- The appliances' synchronization interface ports must be connected either directly, or via a hub or a switch. For example, if the DMZ is the synchronization interface, then the DMZ/WAN2 ports on the appliances must be connected to each other.

  The synchronization interface need not be dedicated for synchronization only. It may be shared with an active internal network or bridge.

You can configure HA for the WAN interface, for any bridge, and for any internal network except wireless networks and the OfficeMode network.

Note: You can enable the DHCP server in all Safe@Office appliances. A Passive Gateway's DHCP server will start answering DHCP requests only if the Active Gateway fails.

Note: If you configure HA for the primary WLAN network:

- A passive appliance's wireless transmitter will be disabled until the gateway becomes active.
- The two primary WLAN networks can share the same SSID and wireless frequency.
- Wireless interfaces cannot serve as the synchronization interface.

Configuring High Availability on a Gateway

Power Pack

The following procedure explains how to configure HA on a single gateway. You must perform this procedure on each Safe@Office appliance that you want to include in the HA cluster.

To configure HA on a Safe@Office appliance

1. Set the appliance's internal IP addresses and network range.

   Each appliance must have a different internal IP address.

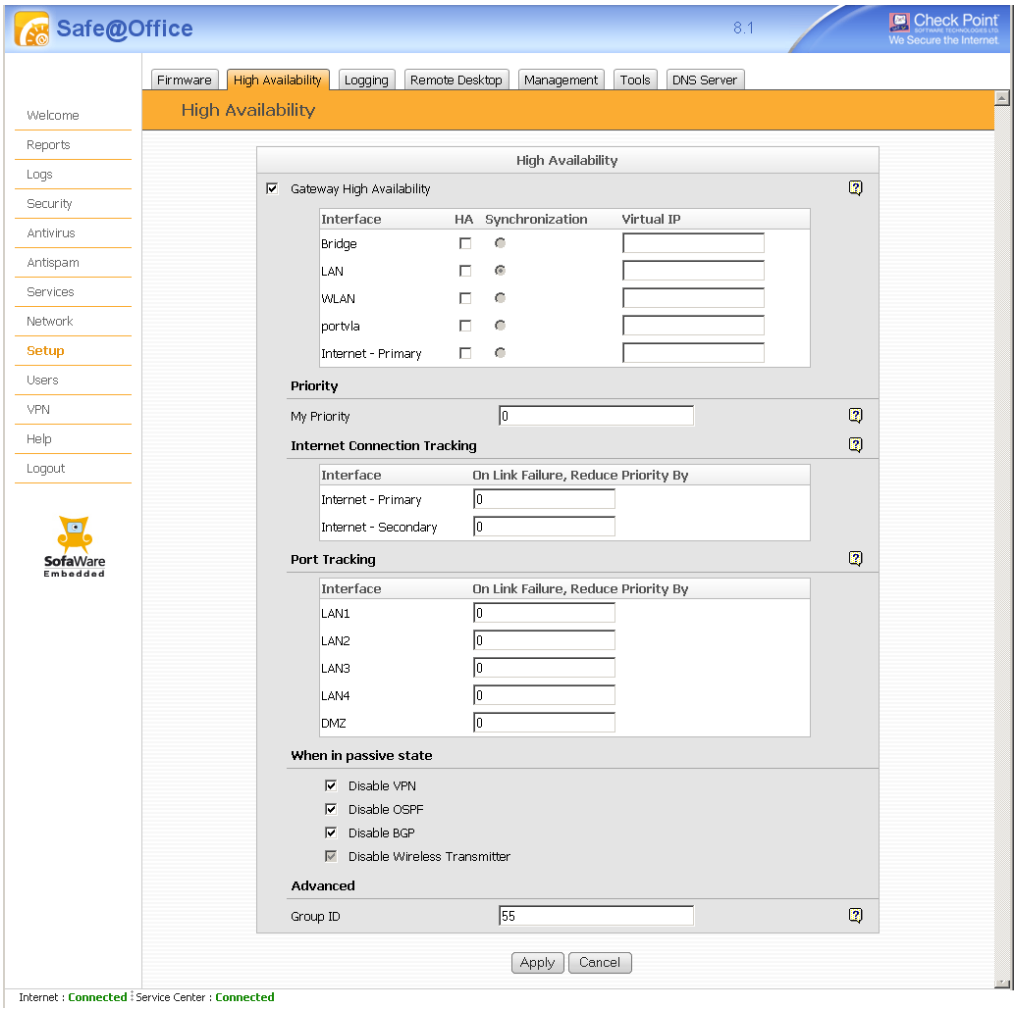
   See ***Changing IP Addresses*** on page 198.

2. Click Setup in the main menu, and click the High Availability tab.

   The High Availability page appears.

3. Select the Gateway High Availability check box.

The fields are enabled.



4. Next to each network for which you want to enable HA, select the HA check box.

   The Internet-Primary field represents the WAN interface, and the Internet-Secondary field represents the WAN2 interface.

5. In the Virtual IP field, type the default gateway IP address.

This can be any unused IP address in the network, and must be the same for all gateways.

You can assign a virtual IP address to any internal interface, as well as to "LAN Static IP" Internet connections (that is, LAN connections for which the Obtain IP address automatically (using DHCP) check box is cleared).

6. Click the Synchronization radio button next to the network you want to use as the synchronization interface.

Note: The synchronization interface must be the same for all gateways, and must always be connected and enabled on all gateways. Otherwise, multiple appliances may become active, causing unpredictable problems.

The synchronization interface cannot be an Internet connection or a wireless interface.

7. Complete the fields using the information the following table.
8. Click Apply.

   A success message appears.
9. If desired, configure WAN HA for both the primary and secondary Internet connection.

   This setting should be the same for all gateways. For further information, see the Do not connect if this gateway is in passive state field in ***Using Internet Setup*** on page 141.
10. If you configured a virtual IP address for the WAN or WAN2 interface, configure the Internet connection to use the "Static IP" connection method.

    See ***Using Internet Setup*** on page 141.

Table 50: High Availability Page Fields

In this field...	Do this...
Priority	
My Priority	Type the gateway's priority. This must be an integer between 1 and 255.
Internet Connection Tracking	
Internet - Primary	Type the amount to reduce the gateway's priority if the primary Internet connection goes down. This must be an integer between 0 and 255.
Internet - Secondary	Type the amount to reduce the gateway's priority if the secondary Internet connection goes down. This must be an integer between 0 and 255. Note: This value is only relevant if you configured a backup connection. For information on configuring a backup connection, see ***Configuring a Backup Internet Connection*** on page 191.
Port Tracking	
LAN1-4	Type the amount to reduce the gateway's priority if the LAN port's Ethernet link is lost. This must be an integer between 0 and 255.
DMZ	Type the amount to reduce the gateway's priority if the DMZ / WAN2 port's Ethernet link is lost. This must be an integer between 0 and 255.

In this field...	Do this...
When in passive state	
Disable VPN	Select this option to specify that VPN connectivity should be disabled when the gateway is a Passive Gateway.
Disable OSPF	Select this option to specify that Open Shortest Path First (OSPF) dynamic routing should be disabled when the gateway is a Passive Gateway.
Disable BGP	Select this option to specify that Border Gateway Protocol (BGP) dynamic routing should be disabled when the gateway is a Passive Gateway.
Disable RIP	Select this option to specify that Routing Information Protocol (RIP) dynamic routing should be disabled when the gateway is a Passive Gateway. This field is only relevant for N series appliances.
Disable Multicast routers	Select this option to specify that Distance Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicast - Sparse-Mode (PIM-SM) multicast routing should be disabled when the gateway is a Passive Gateway. This field is only relevant for N series appliances.
Disable Wireless Transmitter	Indicates that the appliance's wireless transmitter should be disabled when the gateway is a Passive Gateway. This option only appears for wireless appliances, and it cannot be cleared.
Advanced	

In this field…	Do this…
Group ID	If multiple HA clusters exist on the same network segment, type the ID number of the cluster to which the gateway should belong. This must be an integer between 1 and 255. The default value is 55. If only one HA cluster exists, there is no need to change this value.

Sample Implementation on Two Gateways

Power Pack

The following procedure illustrates how to configure HA for the following two Safe@Office gateways, Gateway A and Gateway B:

Table 51: Gateway Details

	Gateway A	Gateway B
Internal Networks	LAN, DMZ	LAN, DMZ
Internet Connections	Primary and secondary	Primary only
LAN Network IP Address	192.169.100.1	192.169.100.2
LAN Network Subnet Mask	255.255.255.0	255.255.255.0
DMZ Network IP Address	192.169.101.1	192.169.101.2
DMZ Network Subnet Mask	255.255.255.0	255.255.255.0

The gateways have two internal networks in common, LAN and DMZ. This means that you can configure HA for the LAN network, the DMZ network, or both. You can use either of the networks as the synchronization interface.

The procedure below shows how to configure HA for both the LAN and DMZ networks. The synchronization interface is the DMZ network, the LAN virtual IP address is 192.168.100.3, and the DMZ virtual IP address is 192.168.101.3. Gateway A is the Active Gateway.

To configure HA for Gateway A and Gateway B

1. Connect the LAN port of Gateways A and B to hub 1.
2. Connect the DMZ port of Gateways A and B to hub 2.
3. Connect the LAN network computers of Gateways A and B to hub 1.
4. Connect the DMZ network computers of Gateways A and B to hub 2.
5. Do the following on Gateway A:
   a. Set the gateway's internal IP addresses and network range to the values specified in the table above.

      See ***Changing IP Addresses*** on page 198.
   b. Click Setup in the main menu, and click the High Availability tab.

      The High Availability page appears.
   c. Select the Gateway High Availability check box.

      The Gateway High Availability area is enabled. The LAN and DMZ networks are listed.
   d. Next to LAN, select the HA check box.
   e. In the LAN network's Virtual IP field, type the default gateway IP address 192.168.100.3.
   f. Next to DMZ, select the HA check box.
   g. In the DMZ network's Virtual IP field, type the default gateway IP address 192.168.101.3.
   h. Click the Synchronization radio button next to DMZ.
   i. In the My Priority field, type "100".

      The high priority means that Gateway A will be the Active Gateway.
   j. In the Internet - Primary field, type "20".

      Gateway A will reduce its priority by 20, if its primary Internet connection goes down.
   k. In the Internet - Secondary field, type "30".

Gateway A will reduce its priority by 30, if its secondary Internet connection goes down.

l. Click Apply.

A success message appears.

6. Do the following on Gateway B:

a. Set the gateway's internal IP addresses and network range to the values specified in the table above.

See ***Changing IP Addresses*** on page 198.

b. Click Setup in the main menu, and click the High Availability tab.

The High Availability page appears.

c. Select the Gateway High Availability check box.

The Gateway High Availability area is enabled. The LAN and DMZ networks are listed.

d. Next to LAN, select the HA check box.

e. In the LAN network's Virtual IP field, type the default gateway IP address 192.168.100.3.

f. Next to DMZ, select the HA check box.

g. In the DMZ network's Virtual IP field, type the default gateway IP address 192.168.101.3.

h. Click the Synchronization radio button next to DMZ.

i. In the My Priority field, type "60".

The low priority means that Gateway B will be the Passive Gateway.

j. In the Internet - Primary field, type "20".

Gateway B will reduce its priority by 20, if its Internet connection goes down.

k. Click Apply.

A success message appears.

Gateway A's priority is 100, and Gateway B's priority is 60. So long as one of Gateway A's Internet connections is up, Gateway A is the Active Gateway, because its priority is higher than that of Gateway B.

If both of Gateway A's Internet connections are down, it deducts from its priority 20 (for the primary connection) and 30 (for the secondary connection), reducing its priority to 50. In this case, Gateway B's priority is the higher priority, and it becomes the Active Gateway.

Chapter 9

Using Traffic Shaper

This chapter describes how to use Traffic Shaper to control the flow of communication to and from your network.

This chapter includes the following topics:

Overview 293
Setting Up Traffic Shaper 295
Predefined QoS Classes 296
Adding and Editing Classes 298
Viewing and Deleting Classes 302
Restoring Traffic Shaper Defaults 303

Overview

Traffic Shaper is a bandwidth management solution that allows you to set bandwidth policies to control the flow of communication. Traffic Shaper ensures that important traffic takes precedence over less important traffic, so that your business can continue to function with minimum disruption, despite network congestion.

Traffic Shaper uses Stateful Inspection technology to access and analyze data derived from all communication layers. This data is used to classify traffic in Quality of Service (QoS) classes. Traffic Shaper divides available bandwidth among the classes according to weight. For example, suppose Web traffic is deemed three times as important as FTP traffic, and these services are assigned weights of 30 and 10 respectively. If the lines are congested, Traffic Shaper will maintain the ratio of bandwidth allocated to Web traffic and FTP traffic at 3:1.

If a specific class is not using all of its bandwidth, the leftover bandwidth is divided among the remaining classes, in accordance with their relative weights. In the example above, if only one Web and one FTP connection are active and they are competing, the Web connection will receive 75% (30/40) of the leftover bandwidth, and the FTP connection will receive 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection will receive 100% of the bandwidth.

Each class has a bandwidth limit, which is the maximum amount of bandwidth that connections belonging to that class may use together. Once a class has reached its bandwidth limit, connections belonging to that class will not be allocated further bandwidth, even if there is unused bandwidth available. For example, traffic used by Peer-To-Peer file-sharing applications may be limited to a specific rate, such as 512 kilobit per second. Each class also has a "Delay Sensitivity" value, indicating whether connections belonging to the class should be given precedence over connections belonging to other classes.

Your Safe@Office appliance offers different degrees of traffic shaping, depending on its model:

- Simplified Traffic Shaper. Includes a fixed set of four predefined classes. You can assign network traffic to each class, but you cannot modify the classes, delete them, or create new classes. Available in Safe@Office 1000N.
- Advanced Traffic Shaper. Includes a set of four predefined classes, but enables you to modify the classes, delete them, and create new classes. You can define up to eight classes, including weight, bandwidth limits, and DiffServ (Differentiated Services) Packet Marking parameters. DiffServ marks packets as belonging to a certain Quality of Service class. These packets are then granted priority on the public network according to their class. Available in Safe@Office products with Power Pack.

Note: You can prioritize wireless traffic from WMM-compliant multimedia applications, by enabling Wireless Multimedia (WMM) for the desired wireless network. See ***Manually Configuring a Wireless Network*** on page *321*.

Setting Up Traffic Shaper

500 1000N

To set up Traffic Shaper

1. Enable Traffic Shaper for the Internet connection, using the procedure ***Using Internet Setup*** on page 141.

   You can enable Traffic Shaper for incoming or outgoing connections.

   - When enabling Traffic Shaper for outgoing traffic:

     Specify a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured upstream speed.
   - When enabling Traffic Shaper for incoming traffic:

     Specify a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured downstream speed.

   It is recommended to try different rates in order to determine which ones provide the best results.

Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary.

2. If you are using a Safe@Office product with Power Pack, you can add QoS classes that reflect your communication needs, or modify the four predefined QoS classes.

   See ***Adding and Editing Classes*** on page 298.

Note: If you are using Safe@Office 1000N, you have Simplified Traffic Shaper, and you cannot add or modify the classes. To add or modify classes, upgrade to Safe@Office with Power Pack, which supports Advanced Traffic Shaper.

3. Use Allow or Allow and Forward rules to assign different types of connections to QoS classes.

   For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing VPN traffic with the Urgent QoS class, then Traffic

Shaper will handle outgoing VPN traffic as specified in the bandwidth policy for the Urgent class.

See ***Adding and Editing Rules*** on page 404.

Note: Traffic Shaper must be enabled for the direction of traffic specified in the rule.

Note: If you do not assign a connection type to a class, Traffic Shaper automatically assigns the connection type to the predefined "Default" class.

Predefined QoS Classes

500 1000N

Traffic Shaper provides the following predefined QoS classes.

To assign traffic to these classes, define firewall rules as described in ***Using Rules*** on page 400.

Table 52: Predefined QoS Classes

Class	Weight	Delay Sensitivity	Useful for
Default	10	Medium (Normal Traffic)	Normal traffic. All traffic is assigned to this class by default.

Class	Weight	Delay Sensitivity	Useful for
Urgent	15	High (Interactive Traffic)	Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet. Note that the weight (amount of bandwidth) allocated to this class is less than the weight allocated to the “Important” class. The "Urgent" class is ideal for delay-sensitive traffic that does not demand a high amount of bandwidth.
Important	20	Medium (Normal Traffic)	Important traffic that requires a high allocation of bandwidth, but which is not exceptionally sensitive to delays. For example, you can prioritize the HTTP traffic of a company's executive officers over other types of traffic, by assigning it to the “Important” class.
Low Priority	5	Low (Bulk Traffic)	Traffic that is not sensitive to long delays, and which does not require a high guaranteed bandwidth. For example, SMTP traffic (outgoing email).

Note: In Simplified Traffic Shaper, these classes cannot be changed.

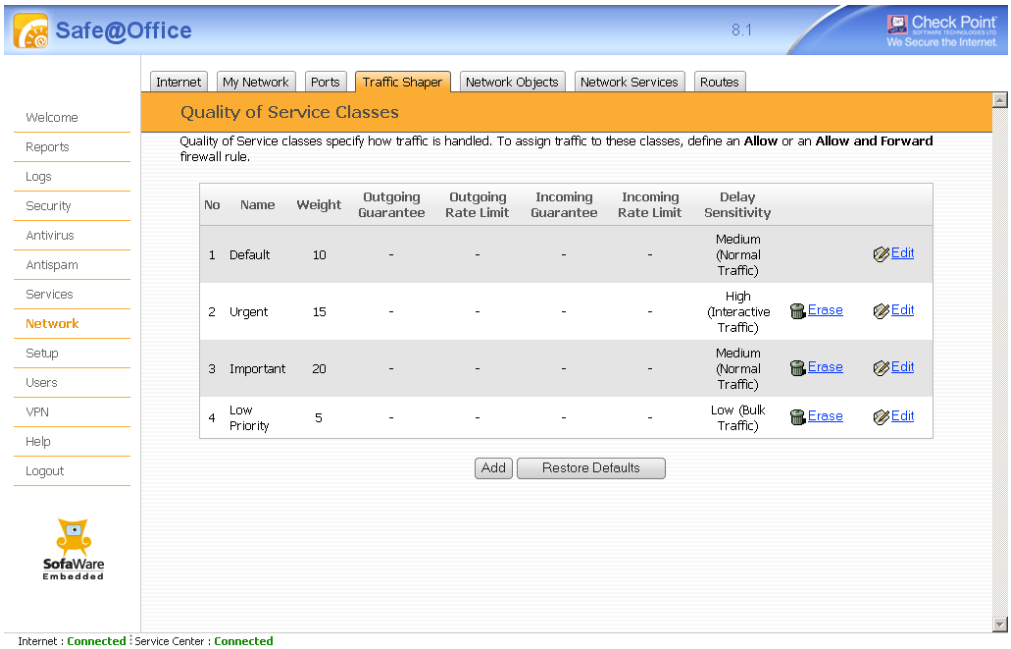
Adding and Editing Classes

Power Pack

To add or edit a QoS class

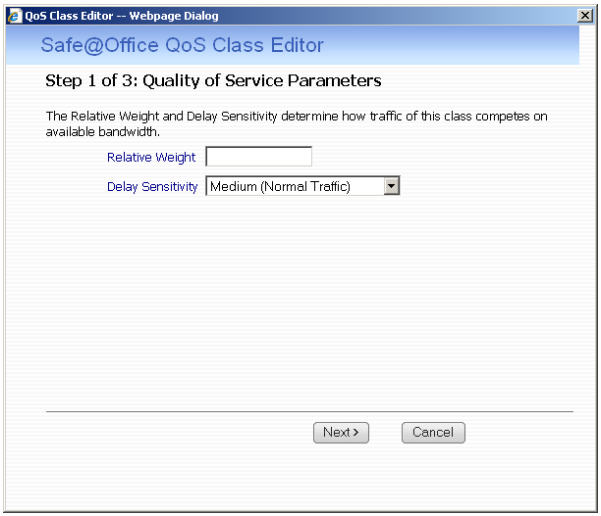
1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.



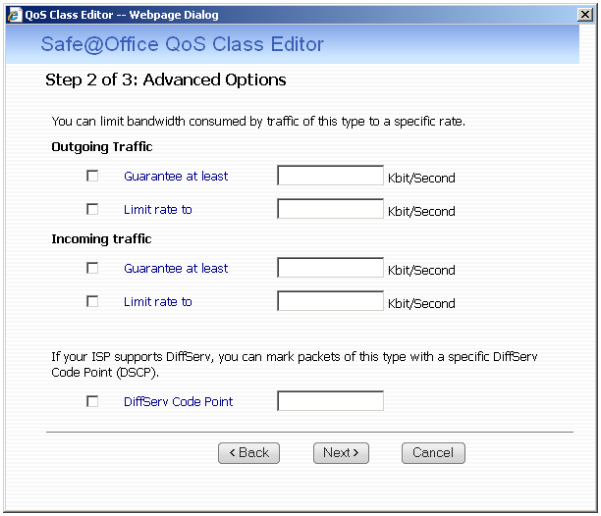
2. Click Add.

The Safe@Office QoS Class Editor wizard opens, with the Step 1 of 3: Quality of Service Parameters dialog box displayed.


QoS Class Editor -- Webpage Dialog
Safe@Office QoS Class Editor
Step 1 of 3: Quality of Service Parameters
The Relative Weight and Delay Sensitivity determine how traffic of this class competes on available bandwidth.
Relative Weight
Delay Sensitivity
Medium (Normal Traffic)
Next >
Cancel

3. Complete the fields using the relevant information in the following table.
4. Click Next.

   The Step 2 of 3: Advanced Options dialog box appears.

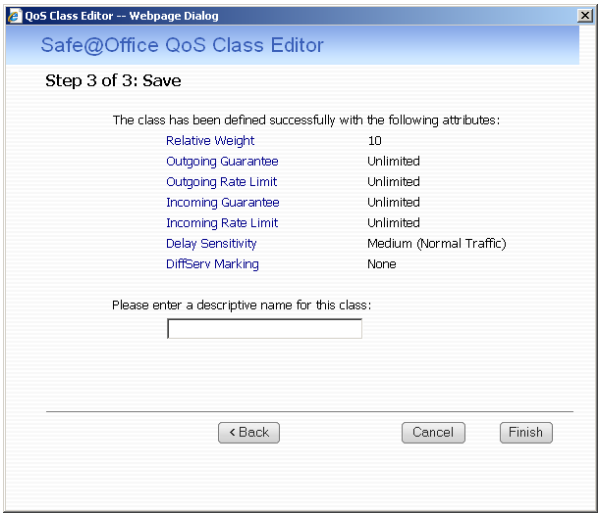

QoS Class Editor -- Webpage Dialog
Safe@Office QoS Class Editor
Step 2 of 3: Advanced Options
You can limit bandwidth consumed by traffic of this type to a specific rate.
Outgoing Traffic
Guarantee at least
Kbit/Second
Limit rate to
Kbit/Second
Incoming traffic
Guarantee at least
Kbit/Second
Limit rate to
Kbit/Second
If your ISP supports DiffServ, you can mark packets of this type with a specific DiffServ Code Point (DSCP).
DiffServ Code Point
< Back
Next >
Cancel

5. Complete the fields using the relevant information in the following table.

Note: Traffic Shaper may not enforce guaranteed rates and relative weights for incoming traffic as accurately as for outgoing traffic. This is because Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on enabling Traffic Shaper for incoming and outgoing traffic, see ***Using Internet Setup*** on page *141*.

6. Click Next.

   The Step 3 of 3: Save dialog box appears with a summary of the class.


QoS Class Editor -- Webpage Dialog
Safe@Office QoS Class Editor
Step 3 of 3: Save
The class has been defined successfully with the following attributes:
Relative Weight 10
Outgoing Guarantee Unlimited
Outgoing Rate Limit Unlimited
Incoming Guarantee Unlimited
Incoming Rate Limit Unlimited
Delay Sensitivity Medium (Normal Traffic)
DiffServ Marking None
Please enter a descriptive name for this class:
< Back
Cancel
Finish

7. Type a name for the class.

   For example, if you are creating a class for high priority Web connections, you can name the class "High Priority Web".

8. Click Finish.

   The new class appears in the Quality of Service Classes page.

Table 53: QoS Class Fields

In this field...	Do this...
Relative Weight	Type a value indicating the class's importance relative to the other defined classes. For example, if you assign one class a weight of 100, and you assign another class a weight of 50, the first class will be allocated twice the amount of bandwidth as the second when the lines are congested.
Delay Sensitivity	Select the degree of precedence to give this class in the transmission queue: • Low (Bulk Traffic) - Traffic that is not sensitive to long delays. For example, SMTP traffic (outgoing email). • Medium (Normal Traffic) - Normal traffic • High (Interactive Traffic) - Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet. Traffic Shaper serves delay-sensitive traffic with a lower latency. That is, Traffic Shaper attempts to send packets with a "High (Interactive Traffic)" level before packets with a "Medium (Normal Traffic)" or "Low (Bulk Traffic)" level.
Outgoing Traffic: Guarantee At Least	Select this option to guarantee a minimum bandwidth for outgoing traffic belonging to this class. Then type the minimum bandwidth (in kilobits/second) in the field provided.
Outgoing Traffic: Limit rate to	Select this option to limit the rate of outgoing traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.
Incoming Traffic: Guarantee At Least	Select this option to guarantee a minimum bandwidth for incoming traffic belonging to this class. Then type the minimum bandwidth (in kilobits/second) in the field provided.

In this field...	Do this...
Incoming Traffic: Limit rate to	Select this option to limit the rate of incoming traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.
DiffServ Code Point	Select this option to mark packets belonging to this class with a DiffServ Code Point (DSCP), which is an integer between 0 and 63. Then type the DSCP in the field provided. The marked packets will be given priority on the public network according to their DSCP. To use this option, your ISP or private WAN must support DiffServ. You can obtain the correct DSCP value from your ISP or private WAN administrator.

Viewing and Deleting Classes

Power Pack

You cannot delete a class that is currently used by a rule. You can determine whether a class is in use or not, by viewing the Rules page.

To view or delete an existing QoS class

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears with a list of all defined QoS classes.

2. To delete a QoS class, do the following:
   a. In the desired class's row, click Erase.
      A confirmation message appears.
   b. Click OK.
      The class is deleted.

Restoring Traffic Shaper Defaults

Power Pack

If desired, you can reset the Traffic Shaper bandwidth policy to use the four predefined classes, and restore these classes to their default settings. For information on these classes and their defaults, see ***Predefined QoS Classes*** on page 296.

Note: This will delete any additional classes you defined in Traffic Shaper and reset all rules to use the Default class.

If one of the additional classes is currently used by a rule, you cannot reset Traffic Shaper to defaults. You can determine whether a class is in use or not, by viewing the Rules page.

To restore Traffic Shaper defaults

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.

2. Click Restore Defaults.

   A confirmation message appears.

3. Click OK.

Chapter 10

Working with Wireless Networks

This chapter describes how to configure wireless internal networks.

This chapter includes the following topics:

Overview 305
Configuring Wireless Networks 314
Troubleshooting Wireless Connectivity 342

Overview

500W 1000NW

Your Safe@Office wireless appliance features a built-in 802.11b/g/n access point that is tightly integrated with the firewall and VPN.

Safe@Office 1000NW wireless appliances support the latest 802.11n standard (up to 300 Mbps) which integrates multiple-input and multiple-output (MIMO) features. MIMO is a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna, and reduces problems with reflected signals. In addition, MIMO includes Spatial Division Multiplexing (SDM), which spatially multiplexes independent data streams that are transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput, as the number of resolved special data streams is increased.

In addition to MIMO, 802.11n also supports 40MHz channels, a channel width that is double the 20MHz available in previous 802.11 PHYs, allowing for doubling of the PHY data rate over a single 20 MHz channel.

Safe@Office 1000NW appliances are backwards compatible with the older 802.11b standard (up to 11 Mbps) and 802.11g standard (up to 54 Mbps), so that both new and old adapters of these standards are interoperable. Safe@Office 500W appliances also support a special Super G mode that allows reaching a throughput of up to 108 Mbps with Super G

compatible stations. For more information on the Super G mode refer to: http://www.super-ag.com.

Safe@Office wireless appliances transmit in 2.4GHz range, using dual diversity antennas to increase the range. When the 802.11n standard is employed with Safe@Office 1000NW, the appliance can transmit in the 5GHz range, as well. Safe@Office 500W appliances support a special extended range (XR) mode that allows up to three times the range of a regular 802.11g access point. XR dramatically stretches the performance of a wireless LAN, by enabling long-range connections. The architecture delivers receive sensitivities of up to 105 dBm, over 20 dB more than the 802.11 specification. This allows ranges of up to 300 meters indoors, and up to 1 km (3200 ft) outdoors, with XR-enabled wireless stations (actual range depends on environment).

The Primary WLAN

500W 1000NW

In addition to the LAN and DMZ networks, you can define a wireless internal network called the primary WLAN (wireless LAN) network. The primary WLAN is the main wireless network, and it controls all other wireless network's statuses: wireless networks can be enabled only if the primary WLAN is enabled, and disabling the primary WLAN automatically disables all other wireless network. In addition, all wireless networks inherit certain settings from the primary WLAN.

You can configure the primary WLAN in either of the following ways:

- Wireless Configuration Wizard. Guides you through the primary WLAN setup, step by step.

  See ***Using the Wireless Configuration Wizard*** on page 314.

- Manual configuration. Offers advanced setup options for the primary WLAN.

  See ***Manually Configuring a WLAN*** on page 321.

Note: If the Safe@Office 1000N Power Pack upgrade is not installed, the primary WLAN is the only wireless network.

Virtual Access Points

500W | 1000NW | Power Pack

The Safe@Office appliance enables you to partition the primary WLAN into virtual access points (VAPs). A VAP is a logical wireless network behind the Safe@Office appliance and is a type of VLAN (see ***Configuring VLANs*** on page 216). Like other types of VLANs, VAPs are isolated from each other and can have separate security policies, IP network segments, and Traffic Shaper settings. This enables you to configure separate policies for different groups of wireless users.

For example, you could assign different permissions to employees and guests using your company's wireless network, by defining two VAPs called “Guest” and “Employee”. The Guest VAP would use simple WPA-Personal encryption, and the security policy would mandate that stations connected to this network can access the Internet, but not sensitive company resources. You could configure Traffic Shaper bandwidth management to give stations in the Guest network a low priority, and by enabling Secure HotSpot on this network, you could define terms of use that the guest users must accept before accessing the Internet. In contrast, the Employee VAP would use the more secure WPA2-Enterprise (802.11i) encryption standard and allow employees to access company resources such as the intranet.

You can configure up to three VAPs, in addition to the primary WLAN. For information on configuring VAPs, see ***Configuring VAPs*** on page 333.

Wireless Distribution System Links

500W | 1000NW | Power Pack

The Safe@Office appliance enables you to extend the primary WLAN's coverage area, by creating a Wireless Distribution System (WDS). A WDS is a system of access points that communicate with each other wirelessly via WDS links, without any need for a wired backbone. For example, if your business has expanded across two buildings, and a single access point no longer provides sufficient coverage, you can add another access point that acts as a repeater. If it is impractical or costly to run wires between the access points, you can connect them by configuring a WDS that includes both access points.

WDS is usually used together with bridge mode to connect the networks behind the access points. For example, if you have two network segments, each of which is served by a

different access point, you can bridge the two network segments over WDS links. The network segments will communicate with each other wirelessly via their access points and act as a single network. For information on bridge mode, see ***Using Bridges*** on page 259.

WDS links are considered a type of VLAN (see ***Configuring VLANs*** on page 216). Therefore, they can have separate security policies, IP network segments, and Traffic Shaper settings.

You can use WDS links to create loop-free topologies, such as a star or tree of access points.

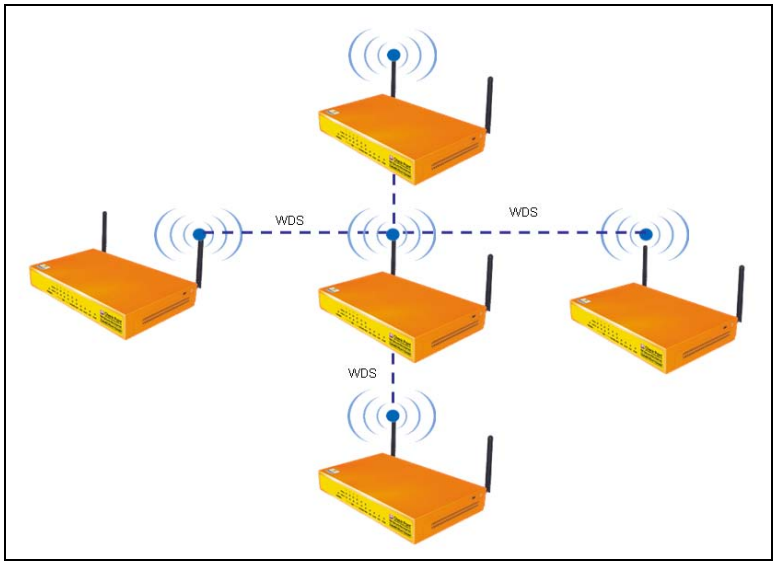


Figure 33: WDS Star of Wireless Access Points

When used together with bridge mode and Spanning Tree Protocol (STP), you can use WDS links to create redundant topologies, such as a loop or mesh of linked access points.

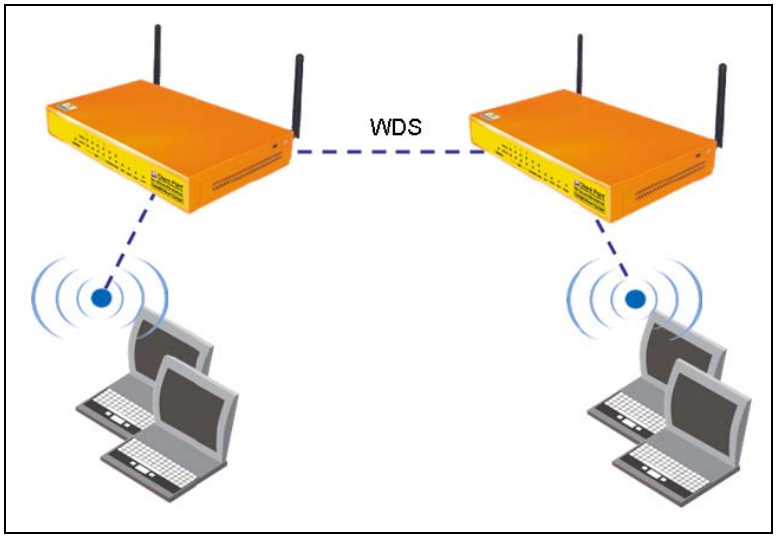


Figure 34: Two Access Points Linked by a WDS Bridge

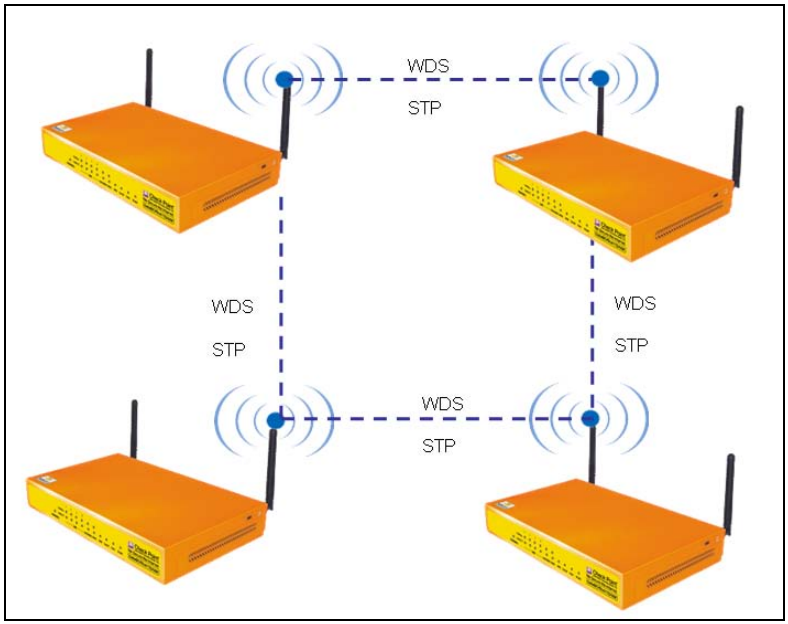


Figure 35: Redundant Loop of Access Points Linked by WDS and STP

Note: Mesh topology is only supported in Safe@Office 500W.

You can configure up to seven WDS links, in addition to the primary WLAN. For information on configuring WDS links, see ***Configuring WDS Links*** on page 338.

Note: All access points in a WDS must use the same radio channel for the WDS link and for communicating with wireless stations. Therefore, using WDS may have a negative impact on wireless throughput. In this case, it is recommended to use a traditional wired backbone to connect the access points, instead of WDS links.

Network Count Limitations

500W | 1000NW | Power Pack

You can configure a total of eight wireless objects, including any combination of the following:

- The primary WLAN
- Up to three virtual access points (VAPs)
- Up to seven WDS links

For example, if you configure the primary WLAN and two VAPs, then you can configure five WDS links, or one more VAP and four WDS links.

When Extended Range (XR) mode is enabled for a wireless object, then it is counted as two objects. For example, if you configure XR mode for the primary WLAN and one VAP, they are counted as four wireless objects.

For information on default security policy rules controlling traffic to and from the primary WLAN and VAPs, see ***Default Security Policy*** on page 393.

Wireless Security Protocols

The Safe@Office wireless security appliance supports the following security protocols:

Table 54: Wireless Security Protocols

Security Protocol	Description
None	No security method is used. This option is not recommended, because it allows unauthorized users to access your wireless network, although you can still limit access from the wireless network by creating firewall rules. This method is suitable for creating public access points.

Security Protocol	Description
WEP encryption	In the WEP (Wired Equivalent Privacy) encryption security method, wireless stations must use a pre-shared key to connect to your network. This method is not recommended, due to known security flaws in the WEP protocol. It is provided for compatibility with existing wireless deployments. Note: The appliance and the wireless stations must be configured with the same WEP key.
802.1x: RADIUS authentication, no encryption	In the 802.1x security method, wireless stations (supplicants) attempting to connect to the access point (authenticator) must first be authenticated, either by a RADIUS server (authentication server) which supports 802.1x, or by the Safe@Office appliance's built-in EAP authenticator. All messages are passed in EAP (Extensible Authentication Protocol). This method is recommended for situations in which you want to authenticate wireless users, but do not need to encrypt the data. This security method is not supported for WDS links. Note: To use this security method, you must first configure either a RADIUS server that supports 802.1x, or set up the network for use with the Safe@Office EAP authenticator. For information on configuring a RADIUS server, see ***Using RADIUS Authentication.*** on page 688 For information on using the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 433.
WPA-Enterprise: RADIUS authentication, encryption	The WPA-Enterprise (Wi-Fi Protected Access) security method uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. Furthermore, WPA-Enterprise includes 802.1x and EAP authentication, based either on a central RADIUS authentication server, or on the Safe@Office appliance's built-in EAP authenticator. This method is

Security Protocol	Description
	recommended for situations where you want to authenticate wireless stations, and to encrypt the transmitted data. Note: To use this security method, you must first configure either a RADIUS server that supports 802.1x, or set up the network for use with the Safe@Office EAP authenticator. For information on configuring a RADIUS server, see ***Using RADIUS Authentication.*** on page 688 For information on using the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 433.
WPA-Personal: password authentication, encryption	The WPA-Personal security method (also called WPA-PSK) is a variation of WPA-Enterprise that does not require an authentication server. WPA-Personal periodically changes and authenticates encryption keys. This is called *rekeying*. This option is recommended for small networks, which want to authenticate and encrypt wireless data, but do not want to install a RADIUS server or use the Safe@Office EAP authenticator. Note: The appliance and the wireless stations must be configured with the same passphrase.
WPA2 (802.11i)	The WPA2 security method uses the more secure Advanced Encryption Standard (AES) cipher, instead of the RC4 cipher used by WPA and WEP. When using WPA-Enterprise or WPA-Personal security methods, the Safe@Office appliance enables you to restrict access to the wireless network to wireless stations that support the WPA2 security method. If this setting is not selected, the Safe@Office appliance allows clients to connect using both WPA and WPA2.

Note: For increased security, it is recommended to enable the Safe@Office internal VPN Server for users connecting from your internal networks, and to install SecuRemote/SecureClient/L2TP/Endpoint Connect on each computer in the wireless network. This ensures that all connections from the wireless network to the LAN are encrypted and authenticated. For information, see ***Internal VPN Server*** on page *606* and ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page *607*.

Configuring Wireless Networks

Note: It is recommended to configure wireless networks via Ethernet and not via a wireless connection, because the wireless connection could be broken after making a change to the configuration.

Using the Wireless Configuration Wizard

500W 1000NW

The Wireless Configuration Wizard provides a quick and simple way of setting up your basic primary WLAN parameters for the first time.

Note: You cannot configure WPA-Enterprise and 802.1x using this wizard. For information on configuring these modes, see ***Manually Configuring a Wireless Network*** on page *321*.

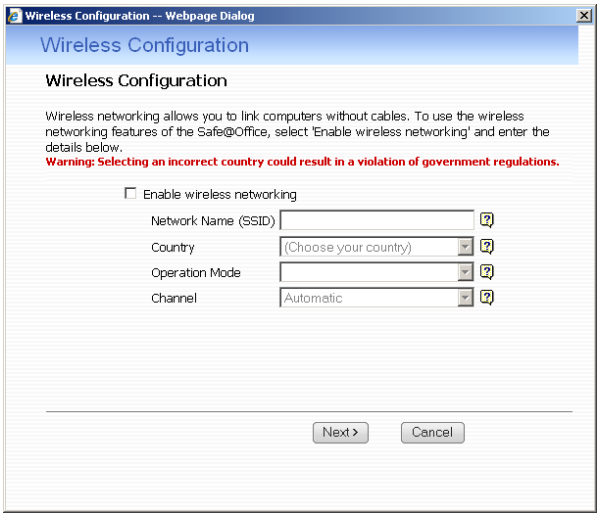
To configure a WLAN using the Wireless Configuration Wizard

1. Prepare the appliance for a wireless connection as described in ***Preparing the Appliance for a Wireless Connection*** on page 102.
2. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
3. In the WLAN network's row, click Edit.

   The Edit Network Settings page appears.
4. Click Wireless Wizard.

The Wireless Configuration Wizard opens, with the Wireless Configuration dialog box displayed.


Wireless Configuration -- Webpage Dialog
Wireless Configuration
Wireless Configuration
Wireless networking allows you to link computers without cables. To use the wireless networking features of the Safe@Office, select 'Enable wireless networking' and enter the details below.
Warning: Selecting an incorrect country could result in a violation of government regulations.
Enable wireless networking
Network Name (SSID)
Country
(Choose your country)
Operation Mode
Channel
Automatic
Next >
Cancel

5. Select the Enable wireless networking check box to enable the primary WLAN.

   The fields are enabled.

6. Complete the fields using the information in ***Basic WLAN Settings Fields*** on page 324.

7. Click Next.

8. The Wireless Security dialog box appears.

Wireless Configuration -- Webpage Dialog
Wireless Configuration
Wireless Security
To secure your wireless network against unwanted intruders, select a wireless security protocol. If you want to create a public, unsecured access point, select None. For additional options and security protocols, you can access the Network > Internal Network tab after completing this wizard.
WPA-Personal (Recommended)
WEP
No Security
To protect your wired LAN from being accessed by wireless users, select Firewall Mode. If you prefer to grant full access from the wireless LAN to the LAN, bypassing firewall protection, select Bridge Mode.
Firewall Mode
Bridge Mode
< Back
Next >
Cancel

9. Do one of the following:

- Click WPA-Personal to use the WPA-Personal security mode.

  WPA-Personal (also called WPA-PSK) uses a passphrase for authentication. This method is recommended for small, private wireless networks, which want to authenticate and encrypt wireless data, but do not want to install a RADIUS server or use the Safe@Office EAP authenticator. Both WPA and the newer, more secure WPA2 (802.11i) will be accepted. To allow only the more secure WPA2 and not WPA, see ***Manually Configuring a WLAN*** on page 321. For larger wireless networks with many users, configure the primary WLAN to use WPA-Enterprise, using the procedure ***Manually Configuring a WLAN*** on page 321.
- Click WEP to use the WEP security mode.

  Using WEP, wireless stations must use a pre-shared key to connect to your network. WEP is widely known to be insecure, and is supported mainly for compatibility with existing networks and stations that do not support other methods.
- Click No Security to use no security to create a public, unsecured access point.

10. Do one of the following:

    - To bridge the LAN and WLAN networks so that they appear as a single unified network, click **Bridge Mode**.

      Traffic from the WLAN to the LAN will be allowed to pass freely, and the LAN and WLAN will share a single IP address range.

      Note: This option creates a bridge called "default-bridge", which includes the WLAN and the LAN. If desired, you can later remove this bridge by running the Wireless Configuration Wizard again, and choosing Firewall Mode. For information on bridges, see ***Using Bridges*** on page *259*.

    - To isolate the LAN from the WLAN, click **Firewall Mode**.

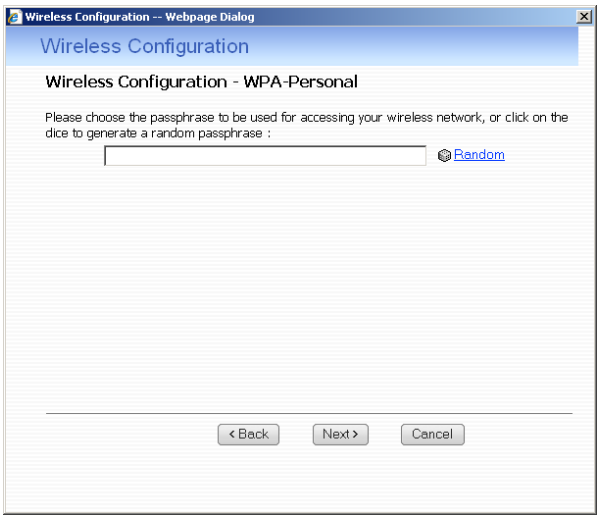
      The WLAN and LAN will be assigned separate, isolated IP networks, and traffic from the WLAN to the LAN will be subjected to the defined firewall policy.

      By default, traffic from the WLAN to the LAN will be blocked, and traffic from the LAN to the WLAN will be allowed. To allow traffic from the WLAN to the LAN, you must create firewall rules. For information, see Using Firewall Rules.

11. Click **Next**.

WPA-Personal

If you chose **WPA-Personal**, the **Wireless Configuration-WPA-Personal** dialog box appears.


Wireless Configuration -- Webpage Dialog
Wireless Configuration
Wireless Configuration - WPA-Personal
Please choose the passphrase to be used for accessing your wireless network, or click on the dice to generate a random passphrase :
Random
< Back
Next >
Cancel

Do the following:

1. In the text box, type the passphrase for accessing the network, or click Random to randomly generate a passphrase.

   This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive.

2. Click Next.

   The Wireless Security Confirmation dialog box appears.

3. Click Next.

4. The **Wireless Security Complete** dialog box appears.

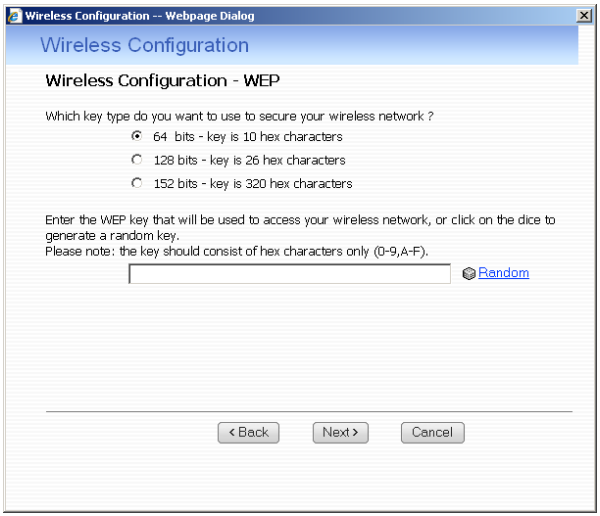
5. Click **Finish**.

   The wizard closes.

6. Prepare the wireless stations.

WEP

If you chose WEP, the Wireless Configuration-WEP dialog box appears.


Wireless Configuration -- Webpage Dialog
Wireless Configuration
Wireless Configuration - WEP
Which key type do you want to use to secure your wireless network ?
64 bits - key is 10 hex characters
128 bits - key is 26 hex characters
152 bits - key is 320 hex characters
Enter the WEP key that will be used to access your wireless network, or click on the dice to generate a random key.
Please note: the key should consist of hex characters only (0-9,A-F).
Random
< Back
Next >
Cancel

Do the following:

1. Choose a WEP key length.

   The possible key lengths are:

   - 64 Bits - The key length is 10 hexadecimal characters.
   - 128 Bits - The key length is 26 hexadecimal characters.
   - 152 Bits - The key length is 32 hexadecimal characters.

   Some wireless card vendors call these lengths 40/104/128, respectively.

   Note that WEP is generally considered to be insecure, regardless of the selected key length.

2. In the text box, type the WEP key, or click Random to randomly generate a key matching the selected length.

   The key is composed of characters 0-9 and A-F, and is not case-sensitive. The wireless stations must be configured with this same key.

3. Click Next.

   The Wireless Security Confirmation dialog box appears.

4. Click Next.

   The Wireless Security Complete dialog box appears.

5. Click Finish.

   The wizard closes.

6. Prepare the wireless stations.

No Security

The Wireless Security Complete dialog box appears.

- Click Finish.

  The wizard closes.

Manually Configuring a Wireless Network

500W 1000NW

To manually configure a wireless network

1. If you intend to use the 802.1x or WPA-Enterprise security mode for the wireless network, do one of the following:

   - To use the Safe@Office EAP authenticator for authenticating wireless clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wireless Clients*** on page 434.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.

   - To use a RADIUS server for authenticating wireless clients, configure a RADIUS server.

     See ***Using RADIUS Authentication*** on page 688.

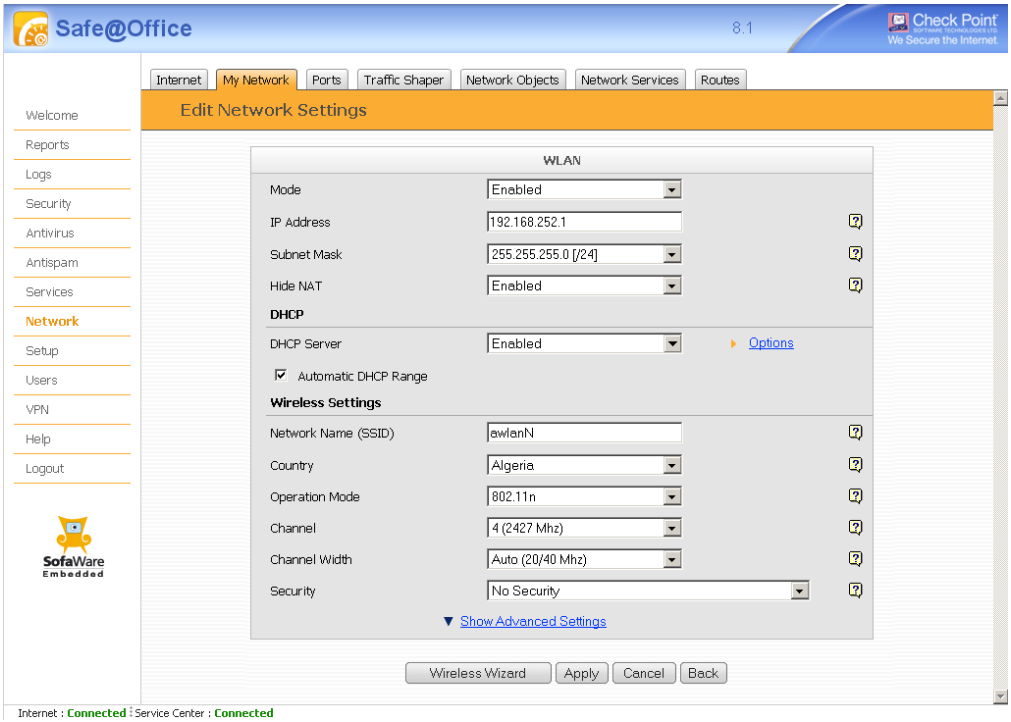
2. Prepare the appliance for a wireless connection as described in ***Preparing the Appliance for a Wireless Connection*** on page 102.

3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

4. In the desired wireless network's row, click Edit.

The Edit Network Settings page appears.



The fields that appear depend on the hardware type.

5. In the Mode drop-down list, select Enabled.

   The fields are enabled.

6. In the IP Address field, type the IP address of the wireless network network's default gateway.

   The wireless network must not overlap other networks.

7. In the Subnet Mask field, type the wireless network's internal network range.

8. If desired, enable or disable Hide NAT.

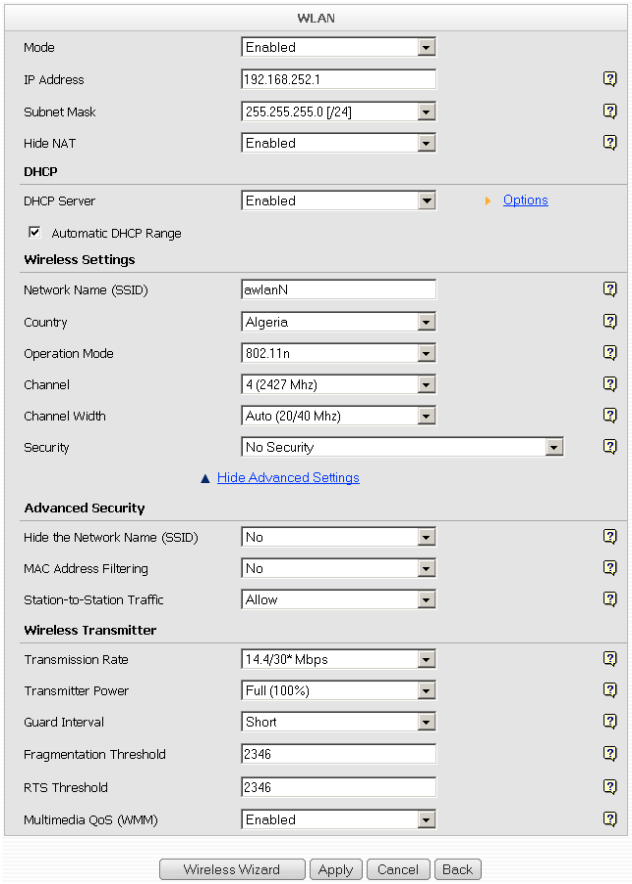
   See ***Enabling/Disabling Hide NAT*** on page 199.

9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 200.

10. Complete the fields using the information in ***Basic Wireless Settings Fields*** on page 324.
11. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced Wireless Settings Fields*** on page 329.

    New fields appear.



    The fields that appear depend on the hardware type.

12. Click Apply.

    A warning message appears, telling you that you are about to change your network settings.

13. Click OK.

    A success message appears.

Note: Some wireless cards have "Infrastructure" and "Ad-hoc" modes. These modes are also called "Access Point" and "Peer to Peer". On the wireless client, choose the "Infrastructure" or "Access Point" mode.
You can set the wireless cards to either "Long Preamble" or "Short Preamble".

Table 55: Basic Wireless Settings Fields

In this field…	Do this…
Wireless Settings	
Network Name (SSID)	Type the network name (SSID) that identifies your wireless network. This name will be visible to wireless stations passing near your access point, unless you enable the Hide the Network Name (SSID) option. It can be up to 32 alphanumeric characters long and is case-sensitive.
Country	Select the country where you are located. Warning: Choosing an incorrect country may result in the violation of government regulations. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
Operation Mode	Select an operation mode: • 802.11b (11 Mbps). Operates in the 2.4 GHz range and offers a maximum theoretical rate of 11 Mbps. When using this mode, only 802.11b stations will be able to connect. • 802.11g (54 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, only 802.11g stations will be able to connect. • 802.11b/g (11/54 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, both 802.11b stations and 802.11g stations will be able to connect.

In this field…	Do this…
	• 802.11g Super (54/108 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.1g stations and 802.11g Super stations will be able to connect. This mode is not available in Safe@Office 1000NW. • 802.11g Super (11/54/108). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.11b stations, 802.11g stations, and 802.11g Super stations will be able to connect. This mode is not available in Safe@Office 1000NW. • 802.11n. Operates in the 5 GHz or 2.4 GHz range, and offers a maximum theoretical rate of 300 Mbps. When using this mode, only 802.11n stations will be able to connect. This mode is only available in Safe@Office 1000NW. • 802.11ng. Operates in the 5 GHz or 2.4 GHz range, and offers a maximum theoretical rate of 300 Mbps. When using this mode, 802.11g stations and 802.11n stations will be able to connect. This mode is only available in Safe@Office 1000NW. The list of modes is dependent on the selected country. You can prevent older wireless stations from slowing down your network, by choosing an operation mode that restricts access to newer wireless stations. Note: The actual data transfer speed is usually significantly lower than the maximum theoretical bandwidth and degrades with distance. Important: The station wireless cards must support the selected operation mode. For a list of cards supporting 802.11g Super, refer to http://www.super-ag.com. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
Channel	Select the radio frequency to use for the wireless connection: • Automatic. The Safe@Office appliance automatically selects a channel. This is the default.

In this field...	Do this...
	• A specific channel. The list of channels is dependent on the selected country and operation mode. Note: If there is another wireless network in the vicinity, the two networks may interfere with one another. To avoid this problem, the networks should be assigned channels that are at least 25 MHz (5 channels) apart. Alternatively, you can reduce the transmission power. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
Channel Width	Select the desired channel width: • Auto (20/40 Mhz). The Safe@Office automatically selects the channel width: 20Mhz or 40Mhz. • 20Mhz Selecting Auto can increase wireless performance, if a 40Mhz channel is available. However, in some cases it may interfere with other access points or wireless equipment in the area. This field is only available in Safe@Office 1000NW.
Security	Select the security protocol to use. For information on the supported security protocols, see ***Wireless Security Protocols*** on page 311. If you select WEP encryption, the WEP Keys area opens. If you select 802.1x, the Authentication Server field appears. If you select WPA-Enterprise, the Authentication Server, Require WPA2 (802.11i), and WPA Encryption fields appear. If you select WPA-Personal, the Passphrase, Require WPA2 (802.11i), and WPA Encryption fields appear. Note: When configuring a WDS link, 802.1x is not supported.

In this field…	Do this…
Authentication Server	Specify which authentication server to use, by selecting one of the following: • RADIUS. A RADIUS server. • Internal User Database. The Safe@Office EAP authenticator.
Passphrase	Type the passphrase for accessing the network, or click Random to randomly generate a passphrase. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive. For the highest security, choose a long passphrase that is hard to guess, or use the Random button. Note: The wireless stations must be configured with this passphrase as well.
Require WPA2 (802.11i)	Specify whether you want to require wireless stations to connect using WPA2, by selecting one of the following: • Enabled. Only wireless stations using WPA2 can access the wireless network. • Disabled. Wireless stations using either WPA or WPA2 can access the wireless network. This is the default.
WPA Encryption	Select the encryption method to use for authenticating and encrypting wireless data: • Auto. The Safe@Office appliance automatically selects the cipher used by the wireless client. This is the default. • AES. Advanced Encryption Standard • TKIP. Temporal Key Integrity Protocol Note: AES is more secure than TKIP; however, some devices do not support AES.

In this field...	Do this...
WEP Keys	If you selected WEP encryption, you must configure at least one WEP key. The wireless stations must be configured with the same key, as well.
Key 1, 2, 3, 4 radio button	Click the radio button next to the WEP key that this gateway should use for transmission. The selected key must be entered in the same key slot (1-4) on the station devices, but the key need not be selected as the transmit key on the stations. Note: You can use all four keys to receive data.
Key 1, 2, 3, 4 length	Select the WEP key length from the drop-down list. The possible key lengths are: • 64 Bits. The key length is 10 characters. • 128 Bits. The key length is 26 characters. • 152 Bits. The key length is 32 characters. Note: Some wireless card vendors call these lengths 40/104/128, respectively. Note: WEP is generally considered to be insecure, regardless of the selected key length.
Key 1, 2, 3, 4 text box	Type the WEP key, or click Random to randomly generate a key matching the selected length. The key is composed of hexadecimal characters 0-9 and A-F, and is not case-sensitive.

Table 56: Advanced Wireless Settings Fields

In this field…	Do this…
Advanced Security	
Hide the Network Name (SSID)	Specify whether you want to hide your network's SSID, by selecting one of the following: • Yes. Hide the SSID. Only devices to which your SSID is known can connect to your network. • No. Do not hide the SSID. Any device within range can detect your network name and attempt to connect to your network. This is the default. Note: Hiding the SSID does not provide strong security, because a determined attacker can still discover your SSID. Therefore, it is not recommended to rely on this setting alone for security.
MAC Address Filtering	Specify whether you want to enable MAC address filtering, by selecting one of the following: • Yes. Enable MAC address filtering. Only MAC addresses that you added as network objects can connect to your network. For information on network objects, see ***Using Network Objects*** on page 227. • No. Disable MAC address filtering. This is the default. Note: MAC address filtering does not provide strong security, since MAC addresses can be spoofed by a determined attacker. Therefore, it is not recommended to rely on this setting alone for security.
Station-to-Station Traffic	Specify whether you want to allow wireless stations on this network to communicate with each other, by selecting one of the following: • Allow. Allow stations to communicate with each other. This is the default. • Block. Block traffic between wireless stations.

In this field...	Do this...
Wireless Transmitter	
Transmission Rate	Select the transmission rate: • Automatic. The Safe@Office appliance automatically selects a rate. This is the default. • A specific rate This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
Transmitter Power	Select the transmitter power. Setting a higher transmitter power increases the access point's range. A lower power reduces interference with other access points in the vicinity. The default value is Full. It is not necessary to change this value, unless there are other access points in the vicinity. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
Guard Interval	Select the guard interval, which is the amount of time between symbol transmissions (in nanoseconds). The guard interval allows reflections from the previous data transmission to settle before transmitting a new symbol. This can have the following values: • Normal. 800ns • Short. 400ns Selecting Short can increase throughput. However, in some cases it can also increase error rate, due to increased sensitivity to RF reflections. This field appears only for Safe@Office 1000NW.

In this field…	Do this…
Antenna Selection	Multipath distortion is caused by the reflection of Radio Frequency (RF) signals traveling from the transmitter to the receiver along more than one path. Signals that were reflected by some surface reach the receiver after non-reflected signals and distort them. Safe@Office appliances avoid the problems of multipath distortion by using an antenna diversity system. To provide antenna diversity, each wireless security appliance has two antennas. Specify which antenna to use for communicating with wireless stations: • Automatic. The Safe@Office appliance receives signals through both antennas and automatically selects the antenna with the lowest distortion signal to use for communicating. The selection is made on a per-station basis. This is the default. • ANT 1. The ANT 1antenna is always used for communicating. • ANT 2. The ANT 2 antenna is always used for communicating. Use manual diversity control (ANT 1 or ANT 2), if there is only one antenna connected to the appliance. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links. This field does not appear for Safe@Office 1000NW.
Fragmentation Threshold	Type the smallest IP packet size (in bytes) that requires that the IP packet be split into smaller fragments. If you are experiencing significant radio interference, set the threshold to a low value (around 1000), to reduce error penalty and increase overall throughput. Otherwise, set the threshold to a high value (around 2000), to reduce overhead. The default value is 2346.

In this field...	Do this...
RTS Threshold	Type the smallest IP packet size for which a station must send an RTS (Request To Send) before sending the IP packet. If multiple wireless stations are in range of the access point, but not in range of each other, they might send data to the access point simultaneously, thereby causing data collisions and failures. RTS ensures that the channel is clear before the each packet is sent. If your network is congested, and the users are distant from one another, set the RTS threshold to a low value (around 500). Setting a value equal to the fragmentation threshold effectively disables RTS. The default value is 2346.
Extended Range Mode (XR)	Specify whether to use Extended Range (XR) mode: • **Disabled.** XR mode is disabled. • **Enabled.** XR mode is enabled. XR will be automatically negotiated with XR-enabled wireless stations and used as needed. This is the default. This field does not appear for Safe@Office 1000NW.
Multimedia QoS (WMM)	Specify whether to use the Wireless Multimedia (WMM) standard to prioritize traffic from WMM-compliant multimedia applications. This can have the following values: • **Disabled.** WMM is disabled. This is the default. • **Enabled.** WMM is enabled. The Safe@Office appliance will prioritize multimedia traffic according to four access categories (Voice, Video, Best Effort, and Background). This allows for smoother streaming of voice and video when using WMM aware applications.

In this field…	Do this…
WDS	Specify whether to enable WDS links: • Disabled. WDS links are disabled. • Enabled. WDS links are enabled. For information on configuring WDS links, see ***Configuring Wireless Distribution System Links*** on page 338. This field appears only for Safe@Office 1000NW.

C onfiguring Virtual Access Points

500W | 1000NW | Power Pack

You can partition the wireless network into wireless VLANs called virtual access points (VAPs). You can use VAPs to grant different permissions to groups of wireless users, by configuring each VAP with the desired security policy and network settings, and then assigning each group of wireless users to the relevant VAP. For more information on VAPs, see ***Overview*** on page 305.

Note: While virtual access points (VAPs) can have different security settings and network names, all VAPs inherit the following wireless settings from the primary WLAN:

- Country
- Operation Mode
- Channel
- Transmission Rate
- Transmitter Power
- Antenna Selection

For information on configuring these settings in the primary WLAN, see ***Manually Configuring a Wireless Network*** on page *321*.

Note: To enable VAPs, you must first enable the primary WLAN network. If you disable the primary WLAN network, all VAPs are automatically disabled.

The procedure below explains how to add or edit a VAP. For information on deleting a VAP, see ***Deleting VLANs*** on page 223.

To add or edit a VAP

1. Configure and enable the primary WLAN.

   For information on configuring the primary WLAN manually, see ***Manually Configuring a Wireless Network*** on page 321.

   For information on using a wizard to configure the primary WLAN, see ***Using the Wireless Wizard*** on page 314.

2. If you intend to use the 802.1x or WPA-Enterprise security mode for the VAP, do one of the following:

   - To use the Safe@Office EAP authenticator for authenticating wireless clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wireless Clients*** on page 434.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.

   - To use a RADIUS server for authenticating wireless clients, configure a RADIUS server.

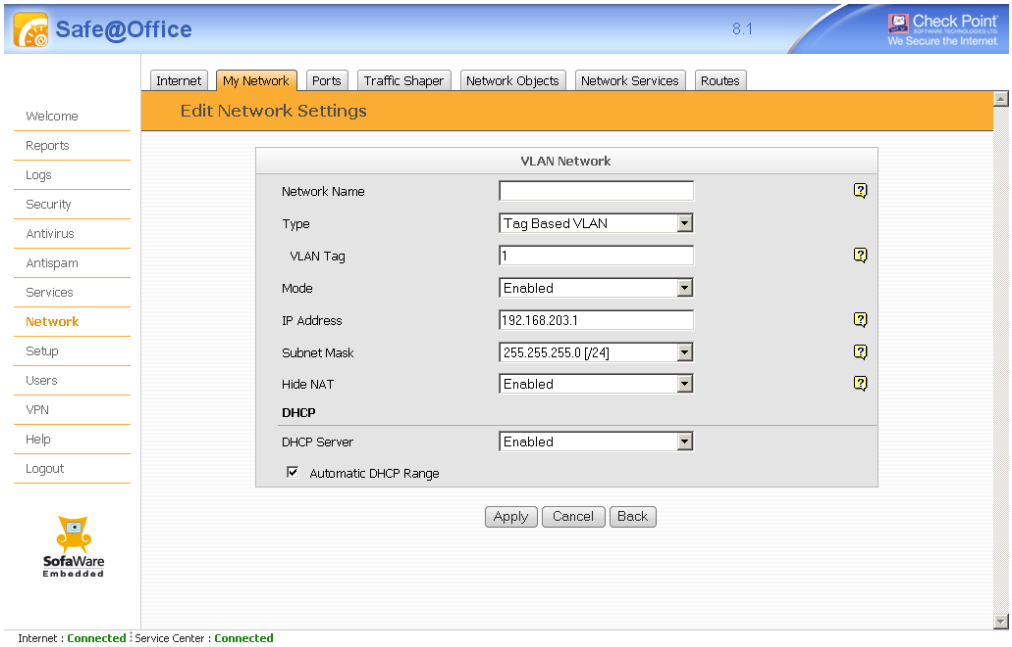
     See ***Using RADIUS Authentication*** on page 688.

3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

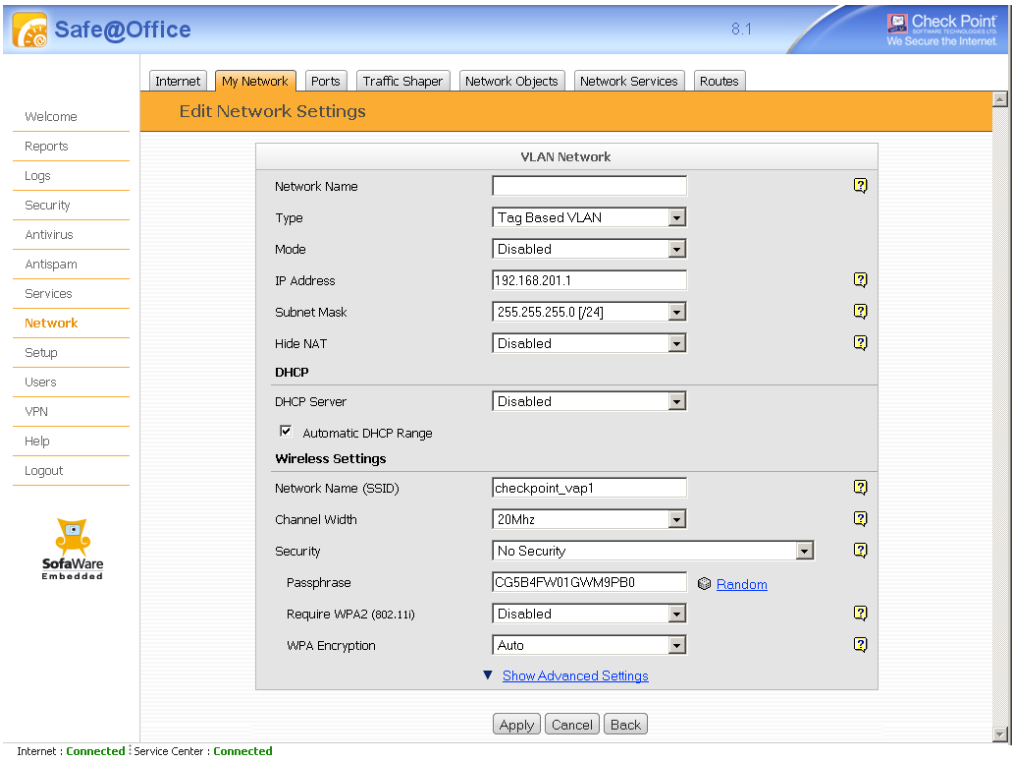
4. Click Add Network.

The Edit Network Settings page appears.



5. In the Network Name field, type a name for the VAP.
6. In the Type drop-down list, select Virtual Access Point.

New fields appear.



The fields that appear depend on the hardware type.

7. In the Mode drop-down list, select Enabled.

   The fields are enabled.

8. In the IP Address field, type the IP address of the VAP network's default gateway.

   The VAP network must not overlap other networks.

9. In the Subnet Mask field, type the VAP's internal network range.

10. If desired, enable or disable Hide NAT.

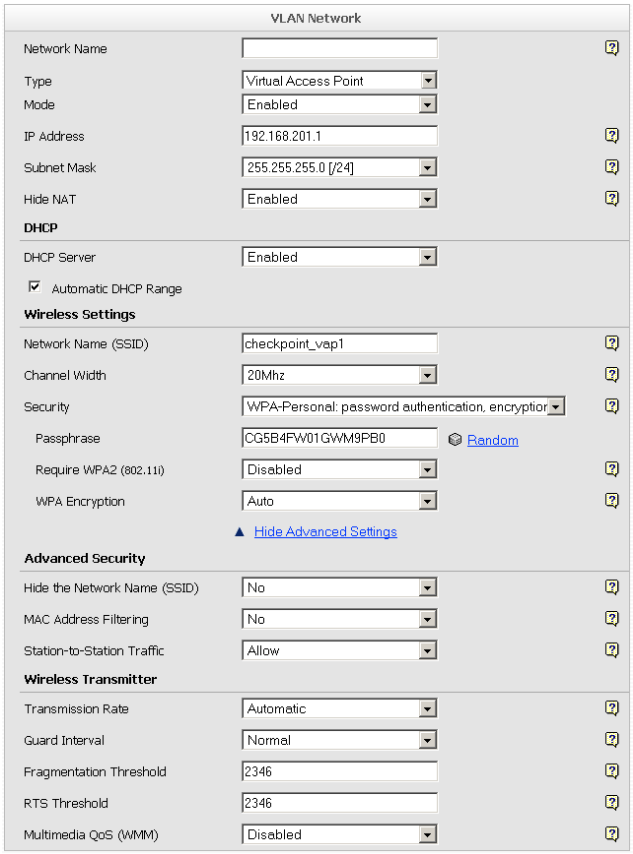
    See ***Enabling/Disabling Hide NAT*** on page 199.

11. If desired, configure a DHCP server.

See ***Configuring a DHCP Server*** on page 200.

12. Complete the fields using the information in ***Basic Wireless Settings Fields*** on page 324.
13. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced Wireless Settings Fields*** on page 329.

    New fields appear.



    The fields that appear depend on the hardware type.

14. Click Apply.

Note: Some wireless cards have "Infrastructure" and "Ad-hoc" modes. These modes are also called "Access Point" and "Peer to Peer". On the wireless client, choose the "Infrastructure" or "Access Point" mode.
You can set the wireless cards to either "Long Preamble" or "Short Preamble".

Configuring Wireless Distribution System Links

500W | 1000NW | Power Pack

You can extend the wireless network across multiple access points, or connect the networks behind different access points, by creating a Wireless Distribution System (WDS). To create a WDS, you must add WDS links between the desired access points.

For more information on WDS links, see ***Overview*** on page 305.

Note: While WDS links can have different security settings, all WDS links inherit the following wireless settings from the primary WLAN:

- Country
- Operation Mode
- Channel
- Transmission Rate
- Transmitter Power
- Antenna Selection
- Security

For information on configuring these settings in the primary WLAN, see ***Manually Configuring a Wireless Network*** on page *321*.

Note: To enable WDS links, you must first enable the primary WLAN network. If you disable the primary WLAN network, all WDS links are automatically disabled.

The procedure below explains how to add or edit a WDS link. For information on deleting a WDS link, see ***Deleting VLANs*** on page 223.

To add or edit a WDS link

1. Configure the primary WLAN as follows:
   a) Enable the primary WLAN.

b) If using Safe@Office1000NW, enable WDS links.

For information on configuring these settings, see ***Manually Configuring a Wireless Network*** on page 321.

2. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

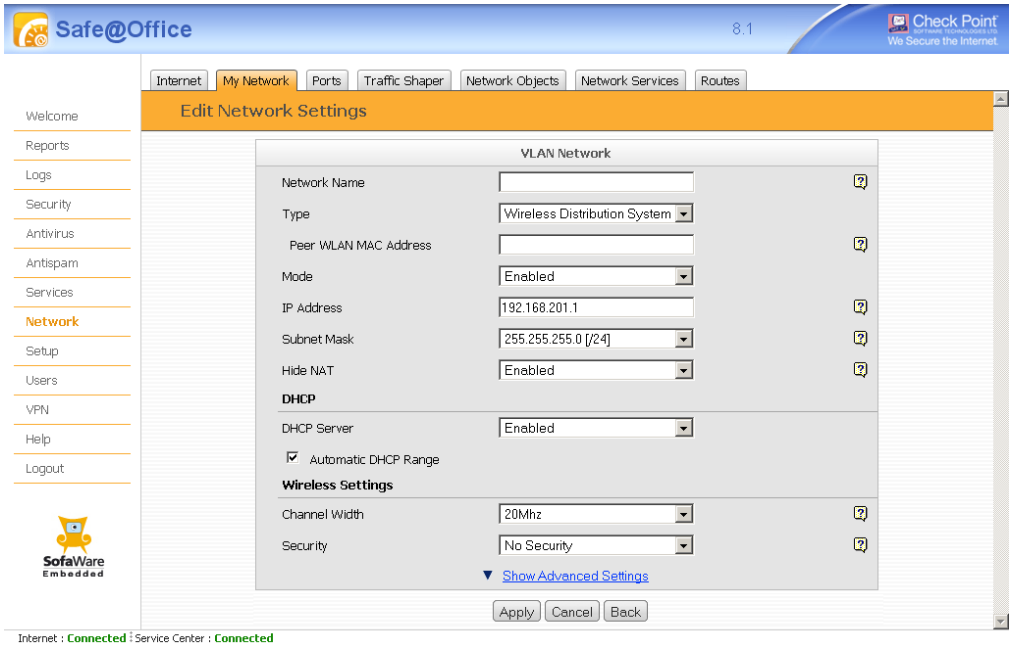
3. Click Add Network.

   The Edit Network Settings page appears.

4. In the Network Name field, type a name for the WDS link.

5. In the Type drop-down list, select Wireless Distribution System.

   New fields appear.



   The fields that appear depend on the hardware type.

6. In the Peer WLAN MAC Address field, type the WLAN MAC address of the access point to which you want to create a WDS link.

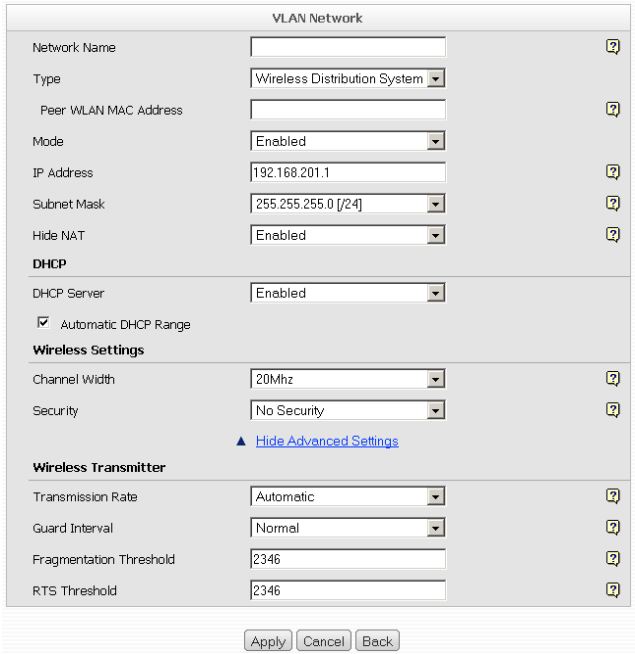
Note: This is the MAC address of the *WLAN* interface, not the WAN MAC address. To see your access point's WLAN MAC address, click Reports in the main menu, and then click Wireless.

7. Do one of the following:
   - To create a bridged WDS link:
     1) In the Mode drop-down list, select Bridged.
        The fields are enabled and additional fields appear.
     2) Complete these fields as described in ***Bridged Network Fields*** on page 273.
   - To create a routed WDS link, do the following:
     1) In the Mode drop-down list, select Enabled.
        The fields are enabled.
     2) In the IP Address field, type the IP address of the WDS link's default gateway.
        The WDS link must not overlap other networks.
     3) In the Subnet Mask field, type the WDS link's internal network range.
8. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 199.
9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 200.
10. Complete the fields using the relevant information in ***Basic Wireless Settings Fields*** on page 324.
11. To configure advanced settings, click Show Advanced Settings and complete the fields using the relevant information in ***Advanced Wireless Settings Fields*** on page 329.

New fields appear.



The fields that appear depend on the hardware type.

12. Click Apply.

Note: Both sides of the WDS link must use the same radio channel and security settings.

Note: The access point can use any supported security protocol to communicate with wireless stations.

Troubleshooting Wireless Connectivity

I cannot connect to a wireless network from a wireless station. What should I do?

- Check that the SSID configured on the station matches the Safe@Office appliance's SSID. The SSID is case-sensitive.
- Check that the encryption settings configured on the station (encryption mode and keys) match the Safe@Office appliance's encryption settings.
- If MAC filtering is enabled, verify that the MAC address of all stations is listed in the Network Objects page (see ***Viewing and Deleting Network Objects*** on page 237).
- Check that the wireless card region matches the access point region.
- Check the wireless card supports the wireless standard that you configured.

I cannot connect to an access point over a WDS link. What should I do?

- Check that both sides of the WDS link are configured with their peer's WLAN MAC address (and not the WAN MAC address).
- Check that both sides of the WDS link are configured to use the same radio channel and security settings.
- Make sure that the peer access points are not too far apart for proper reception.

How do I test wireless reception?

- Look at the Wireless page, and check for excessive errors or dropped packets.
- Look at the My Computers page, to see information for specific wireless stations, such as the number of transmission errors, and the current reception power of each station.
- On the wireless station, open a command window and type ping my.firewall. If you see a large number of dropped packets, you are experiencing poor reception.

Wireless reception is poor. What should I do?

- Adjust the angle of the antennas, until the reception improves. The antennas radiate horizontally in all directions.
- If both antennas are connected to the Safe@Office appliance, check that the Antenna Selection parameter in the primary WLAN's advanced settings is set to Automatic (see ***Manually Configuring a Wireless Network*** on page 321).

- Relocate the Safe@Office appliance to a place with better reception, and avoid obstructions, such as walls and electrical equipment. For example, try mounting the appliance in a high place with a direct line of sight to the wireless stations.
- Check for interference with nearby electrical equipment, such as microwave ovens and cordless or cellular phones.
- Check the Transmission Power parameter in the primary WLAN's advanced settings.
- Make sure that you are not using two access points in close proximity and on the same frequency. For minimum interference, channel separation between nearby access points must be at least 25 MHz (5 channels).
- The Safe@Office appliance supports XR (Extended Range) technology. For best range, enable XR mode in the wireless network's advanced settings, and use XR-enabled stations.
- Range outdoors is normally much higher than indoors, depending on environmental conditions.

Note: You can observe any changes in the wireless reception in the My Computers page. Make sure to refresh the page after making a change.

Note: Professional companies are available for help in setting up reliable wireless networks, with access to specialized testing equipment and procedures.

There are excessive collisions between wireless stations. What should I do?

If you have many concurrently active wireless stations, there may be collisions between them. Such collisions may be the result of a "hidden node" problem: not all of the stations are within range of each other, and therefore are "hidden" from one another. For example, if station A and station C do not detect each other, but both stations detect and are detected by station B, then both station A and C may attempt to send packets to station B simultaneously. In this case, the packets will collide, and Station B will receive corrupted data.

The solution to this problem lies in the use of the RTS protocol. Before sending a certain size IP packet, a station sends an RTS (Request To Send) packet. If the recipient is not currently receiving packets from another source, it sends back a CTS (Clear To Send) packet, indicating that the station can send the IP packet. Try setting the RTS Threshold

parameter in the wireless network's advanced settings to a lower value. This will cause stations to use RTS for smaller IP packets, thus decreasing the likeliness of collisions.

In addition, try setting the Fragmentation Threshold parameter in the wireless network's advanced settings to a lower value. This will cause stations to fragment IP packets of a certain size into smaller packets, thereby reducing the likeliness of collisions and increasing network speed.

Note: Reducing the RTS Threshold and the Fragmentation Threshold too much can have a negative impact on performance.

Note: Setting an RTS Threshold value equal to the Fragmentation Threshold value effectively disables RTS.

I am not getting the full speed. What should I do?

- The actual speed is always less than the theoretical speed, and degrades with distance.
- Read the section about reception problems. Better reception means better speed.
- Check that all your wireless stations support the wireless standard you are using (802.11g or 802.11g Super), and that this standard is enabled in the station software. Transmission speed is determined by the slowest station associated with the access point. For a list of wireless stations that support 802.11g Super, see www.super-ag.com.

Chapter 11

Viewing Reports

This chapter describes the Safe@Office Portal reports.

This chapter includes the following topics:

Viewing the Safe@Office Appliance Status....345
Using the Traffic Monitor....352
Viewing Computers....357
Viewing Connections....359
Viewing Network Statistics....362
Viewing the Routing Table....374
Viewing Wireless Station Statistics....376

Viewing the Safe@Office Appliance Status

500 1000N

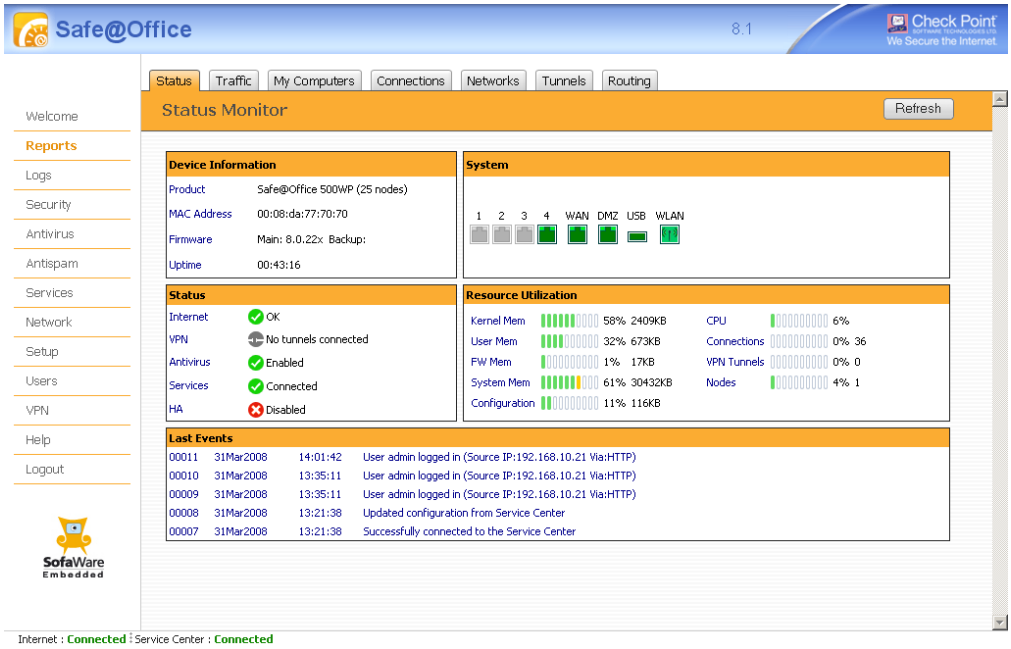
The Safe@Office Status Monitor provides a snapshot of the Safe@Office appliance's current status, enabling you to view the following information in a single glance:

- General appliance information
- Appliance module statuses
- Appliance port statuses
- Resource utilization information
- Recent logged events

To view the Safe@Office appliance's current status

1. Click Reports in the main menu, and click the Status tab.

   The Status Monitor page appears.



   The page displays the information in the following table.

2. To refresh the display, click Refresh.

Table 57: Status Monitor Fields

This field…	Displays…
Device Information	Information about the Safe@Office appliance.
Product	The licensed software and the number of allowed nodes.
MAC Address	The Safe@Office appliance's WAN MAC address.
Firmware	The currently installed firmware: • Main. The version of the primary firmware • Backup. The version of the backup firmware
Uptime	The time that elapsed from the moment the unit was turned on
System	A diagram of the Safe@Office appliance's ports, indicating the ports' statuses. Ports that are currently in use appear in green.
Cellular Modems	Information about connected cellular modems, including the following: • An icon indicating whether the modem is connected to the Internet ( ) or not ( ) • The modem model name • The modem's access technology • A bar graph indicating the current signal strength • The cellular operator’s name You can mouse over the field to view the modem manufacturer, model number, and access technology value, and current signal strength in dBm.
Status	Information about the Safe@Office appliance's status.

<table>
<tr><th>This field...</th><th>Displays...</th></tr>
<tr><td>Internet</td><td>The Safe@Office appliance's overall Internet connection status. This can be any of the following:<table><tr><th>Icon</th><th>Description</th></tr><tr><td> </td><td>OK. One or both Internet connections are connected.</td></tr><tr><td> </td><td>Idle. Both Internet connections are in “idle” state.</td></tr><tr><td> </td><td>Disabled. Both Internet connections are disabled.</td></tr><tr><td> </td><td>Connected with problems. One Internet connection is connected, and the other Internet connection is in “Establishing Connection” state.</td></tr><tr><td> </td><td>No connectivity. All enabled Internet connections are in “Establishing Connection” state.</td></tr></table>For information on individual Internet connections' statuses, see Status Bar on page 121.</td></tr>
<tr><td>VPN</td><td>The Safe@Office appliance's VPN tunnel status. This can be any of the following:<table><tr><th>Icon</th><th>Description</th></tr><tr><td> </td><td>No tunnels connected. There are no open VPN tunnels.</td></tr><tr><td> </td><td>Tunnels are established. There are open VPN tunnels.</td></tr><tr><td> </td><td>Some permanent tunnels are down. Some permanent VPN tunnels are currently down. To view VPN tunnels, click on the link.</td></tr></table></td></tr>
</table>

<table>
<tr><th>This field...</th><th>Displays...</th></tr>
<tr><td>Antivirus</td><td>The Safe@Office appliance's VStream Antivirus status. This can be any of the following:
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td> </td><td>Antivirus enabled. VStream Antivirus is enabled.</td></tr>
<tr><td> </td><td>Antivirus disabled. VStream Antivirus is disabled.</td></tr>
<tr><td> </td><td>Antivirus is enabled but no database is installed. VStream Antivirus is enabled; however, the VStream Antivirus databases are not installed.</td></tr>
</table></td></tr>
<tr><td>Services</td><td>The Safe@Office appliance's Service Center connection status. This can be any of the following:
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td> </td><td>Connected. The Safe@Office appliance is connected to the Service Center, and security services are active.</td></tr>
<tr><td> </td><td>Firmware download: x% completed. The Safe@Office appliance is currently downloading a firmware file from the Service Center. The download is x% complete.</td></tr>
<tr><td> </td><td>Disabled. You are not subscribed to a Service Center.</td></tr>
<tr><td> </td><td>Expired. Your subscription to security services has expired.</td></tr>
<tr><td> </td><td>Failed to connect. The Safe@Office appliance failed to connect to the Service Center.</td></tr>
</table></td></tr>
</table>

This field...	Displays...
HA	The Safe@Office appliance's High Availability status. This can be any of the following: **Icon** — **Description** Passive. High Availability is enabled, and this appliance is a Passive Gateway. Master. High Availability is enabled, and this appliance is the Active Gateway. Disabled. High Availability is disabled.
Resource Utilization	Safe@Office appliance resource utilization information. A bar graph next to each resource indicates the amount currently consumed.
Kernel Mem	The percentage of used memory in the kernel module, followed by the amount in kilobytes.
User Mem	The percentage of used memory in the user module, followed by the amount in kilobytes.
FW Mem	The percentage of used memory in the firewall module, followed by the amount in kilobytes.

This field…	Displays…
System Mem	The percentage of system memory in use, followed by the amount in kilobytes.
Configuration	The percentage of configuration storage space in use out of the total amount of space allocated for configuration storage, followed by the amount in kilobytes.
CPU	The percentage of CPU in use.
Connections	The percentage of established connections out of the licensed number of connections, followed by the number of established connections.
VPN Tunnels	The percentage of established VPN tunnels out of the licensed number of VPN tunnels, followed by the number of established VPN tunnels.
Nodes	The percentage of nodes in use out of the licensed number of nodes, followed by the number of nodes in used.
Last Events	The last five messages logged to the Event Log.

Using the Traffic Monitor

500 1000N

You can view incoming and outgoing traffic for selected network interfaces and QoS classes using the Traffic Monitor. This enables you to identify network traffic trends and anomalies, and to fine tune Traffic Shaper QoS class assignments.

The Traffic Monitor displays separate bar charts for incoming traffic and outgoing traffic, and displays traffic rates in kilobits/second. If desired, you can change the number of seconds represented by the bars in the charts, using the procedure ***Configuring Traffic Monitor Settings*** on page 354.

In network traffic reports, the traffic is color-coded as described in the following table. In the All QoS Classes report, the traffic is color-coded by QoS class.

Table 58: Traffic Monitor Color Coding for Networks

Traffic marked in this color…	Indicates…
Blue	VPN-encrypted traffic
Red	Traffic blocked by the firewall
Green	Traffic accepted by the firewall

You can export a detailed traffic report for all enabled networks and all defined QoS classes, using the procedure ***Exporting General Traffic Reports*** on page 356.

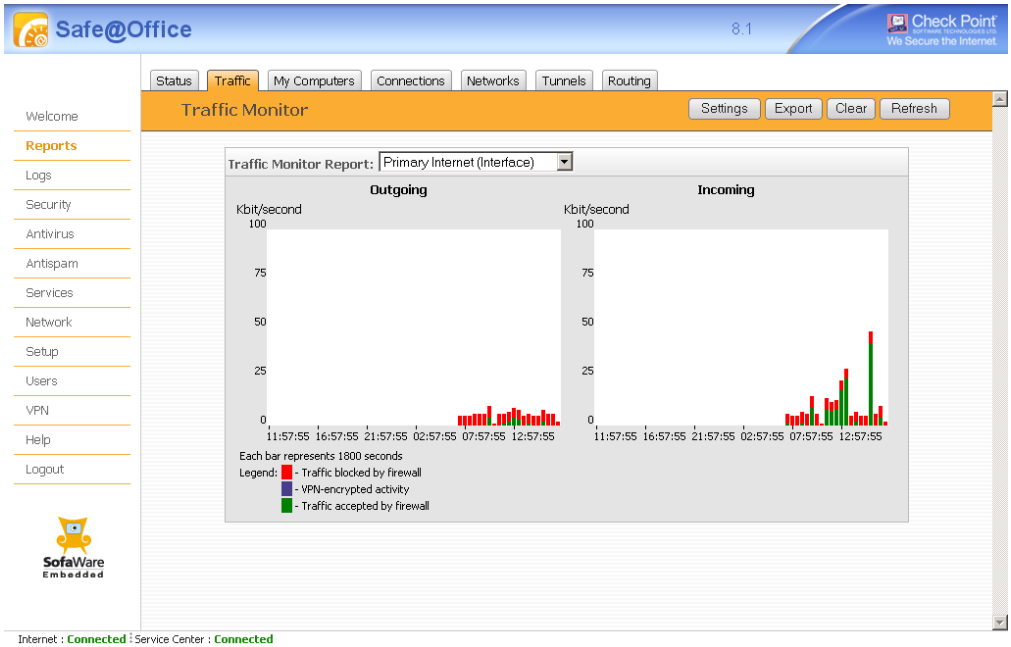
Viewing Traffic Reports

500 1000N

To view a traffic report

1. Click Reports in the main menu, and click the Traffic tab.

   The Traffic Monitor page appears.



2. In the Traffic Monitor Report drop-down list, select the network interface for which you want to view a report.

   The list includes all currently enabled networks. For example, if the DMZ network is enabled, it will appear in the list.

   If Traffic Shaper is enabled, the list also includes the defined QoS classes. Choose All QoS Classes to display a report including all QoS classes. For information on enabling Traffic Shaper see ***Using Internet Setup*** on page 141.

   The selected report appears in the Traffic Monitor page.

3. To refresh all traffic reports, click Refresh.
4. To clear all traffic reports, click Clear.

Note: The firewall blocks broadcast packets used during the normal operation of your network. This may lead to a certain amount of traffic of the type "Traffic blocked by firewall" that appears under normal circumstances and usually does not indicate an attack.

Configuring Traffic Monitor Settings

500 1000N

You can configure the interval at which the Safe@Office appliance should collect traffic data for network traffic reports.

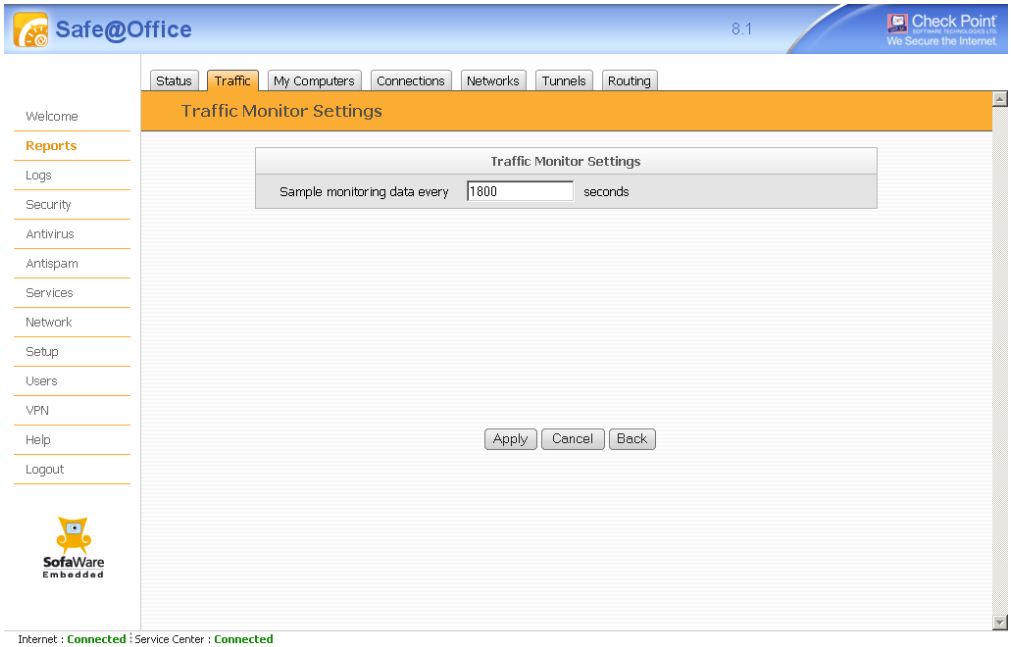
To configure Traffic Monitor settings

1. Click Reports in the main menu, and click the Traffic tab.

   The Traffic Monitor page appears.

2. Click Settings.

The Traffic Monitor Settings page appears.



3. In the Sample monitoring data every field, type the interval (in seconds) at which the Safe@Office appliance should collect traffic data.

   The default value is one sample every 1800 seconds (30 minutes).

4. Click Apply.

Exporting General Traffic Reports

500 1000N

You can export a general traffic report that includes information for all enabled networks and all defined QoS classes to a *.csv (Comma Separated Values) file. You can open and view the file in Microsoft Excel.

To export a general traffic report

1. Click Reports in the main menu, and click the Traffic tab.

   The Traffic Monitor page appears.

2. Click Export.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the configuration file and click Save.

   A *.csv file is created and saved to the specified directory.

Viewing Computers

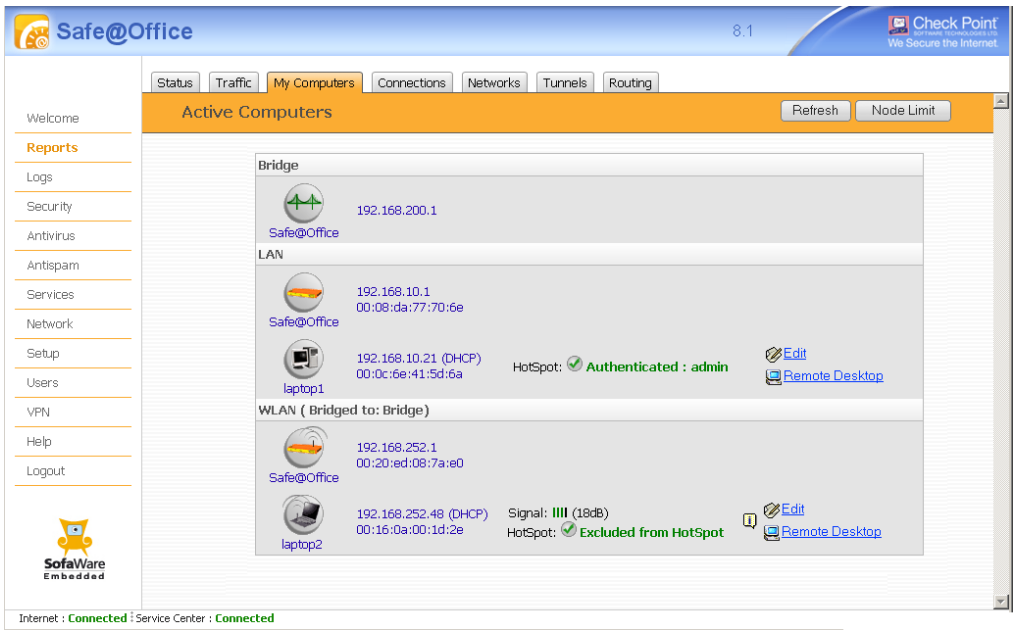
500 1000N

This option allows you to view the currently active computers on your network. The computers are graphically displayed, each with its name, IP address, and settings (DHCP, Static, etc.). You can also view node limit information.

To view the computers

1. Click Reports in the main menu, and click the My Computers tab.

   The Active Computers page appears.



If you configured High Availability, both the master and backup appliances are shown. If you configured OfficeMode, the OfficeMode network is shown.

If there are wireless networks, the wireless stations are shown under the network to which they are connected. For information on viewing statistics for these computers, see ***Viewing Wireless Station Statistics*** on page 376. If a wireless station has been

blocked from accessing the Internet through the Safe@Office appliance, the reason why it was blocked is shown in red.

If a network is bridged, the bridge's name appears in parentheses next to the network's name.

If you are exceeding the maximum number of computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red. These computers are still protected, but they are blocked from accessing the Internet through the Safe@Office appliance.

Note: Computers that did not communicate through the firewall are not counted for node limit purposes, even though they are protected by the firewall and appear in the Active Computers table.

Note: To increase the number of computers allowed by your license, you can upgrade your product. For further information, see ***Upgrading Your Software Product*** on page *722*.

If Secure HotSpot is enabled for some networks, each computer's HotSpot status is displayed next to it. The possible statuses include:

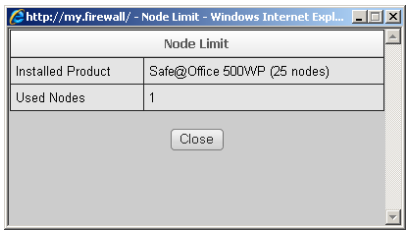
- Authenticated. The computer is logged in to My HotSpot.
- Not Authenticated. The computer is not logged in to My HotSpot.
- Excluded from HotSpot. The computer is in an IP address range excluded from HotSpot enforcement. To enforce HotSpot, you must edit the network object. See ***Adding and Editing Network Objects*** on page 229.

If Remote Desktop is enabled, a link appears next to each computer, enabling you to access its desktop remotely. For information on using Remote Desktop, see ***Using Remote Desktop*** on page 699.

Next to each computer, an Add button enables you to add a network object for the computer, or an Edit button enables you to edit an existing network object for the computer. For information on adding and editing network objects, see ***Adding and Editing Network Objects*** on page 229.

2. To refresh the display, click Refresh.
3. To view node limit information, do the following:
   a. Click Node Limit.

The Node Limit window appears with installed software product and the number of nodes used.



b. Click Close to close the window.

Viewing Connections

500 1000N

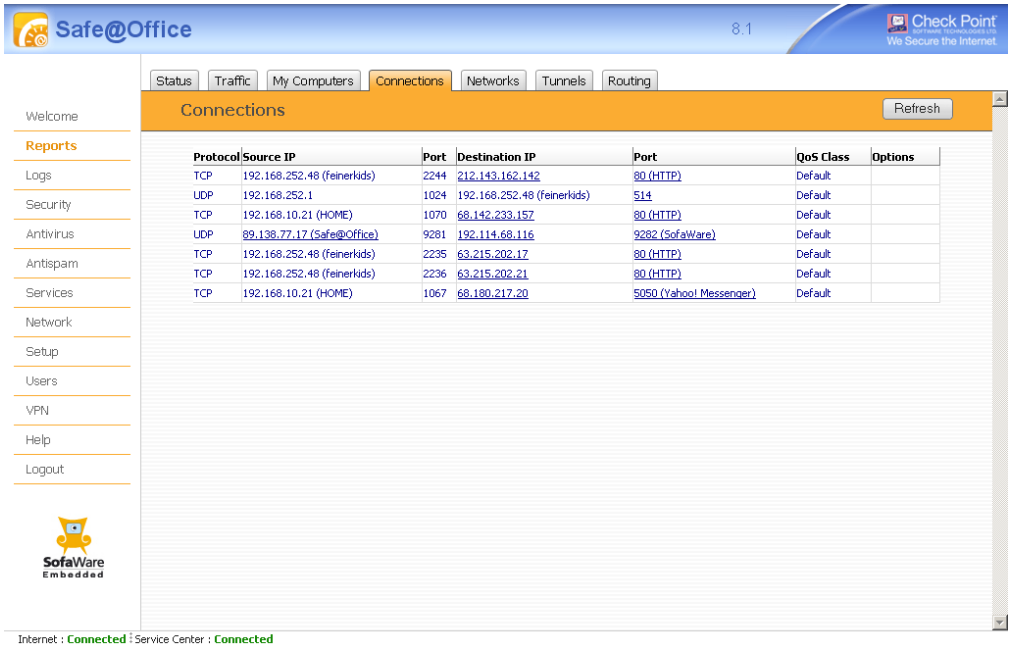
This option allows you to view currently active connections between your networks, as well as those from your networks to the Internet.

Note: The report does not display connections between bridged networks, where Firewall Between Members is disabled.

To view the active connections

1. Click Reports in the main menu, and click the Connections tab.

The Connections page appears.



The page displays the information in the following table.

2. To view information about a destination machine, click its IP address.

   The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to which the IP address is registered and their contact information.

3. To view information about a destination port, click the port.

   A window opens displaying information about the port.

4. To resize a column, drag the relevant column divider right or left.

5. To refresh the display, click Refresh.

Table 59: Connections Fields

This field…	Displays…
Protocol	The protocol used (TCP, UDP, and so on)
Source IP	The source IP address.
Port	The source port
Destination IP	The destination IP address.
Port	The destination port.
QoS Class	The QoS class to which the connection belongs (if Traffic Shaper is enabled)
Options	An icon indicating further details: • - The connection is encrypted. • - The connection is being scanned by VStream Antivirus. • - The connection is being scanned by VStream Antispam.

Viewing Network Statistics

500 1000N

You can view statistics for each of the Safe@Office appliance's Internet connections, internal networks and bridges, using the Network Interface Monitor.

Viewing General Network Statistics

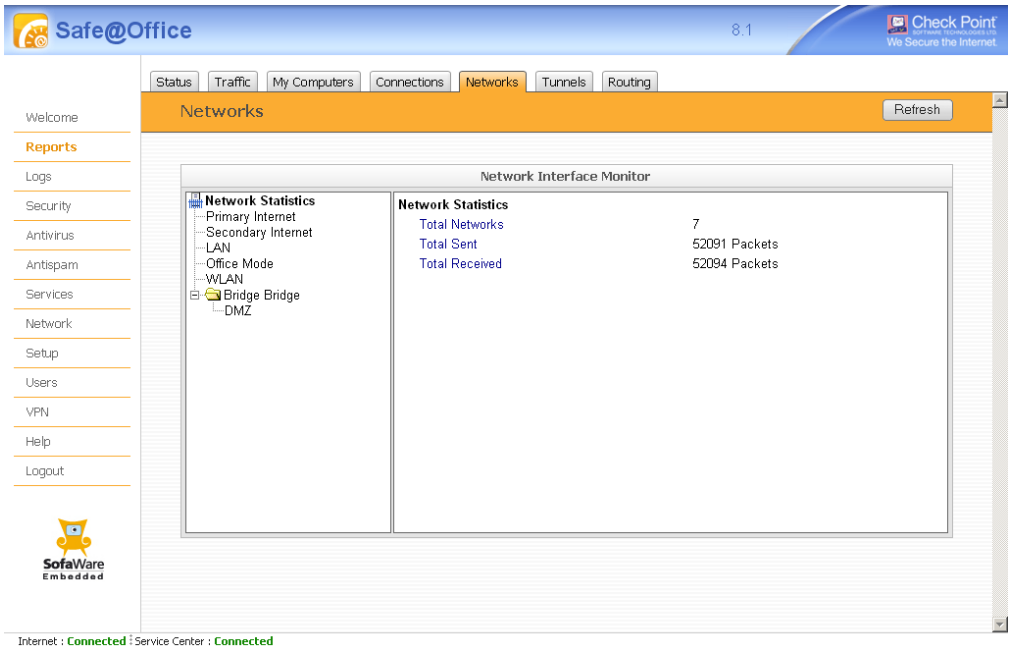
500 1000N

You can view general statistics for the Safe@Office appliance's network interfaces.

To view general network statistics

1. Click Reports in the main menu, and click the Networks tab.

   The Networks page appears displaying general network statistics. For information on the fields, see the following table.



2. To refresh the display, click Refresh.

Table 60: General Network Statistics

This field…	Displays…
Total Networks	The total number of internal networks.
Total Sent	The total number of sent packets on all network interfaces.
Total Received	The total number of received packets on all network interfaces.

Viewing Internet Connection Statistics

500 1000N

You can view statistics for the primary and secondary Internet connections.

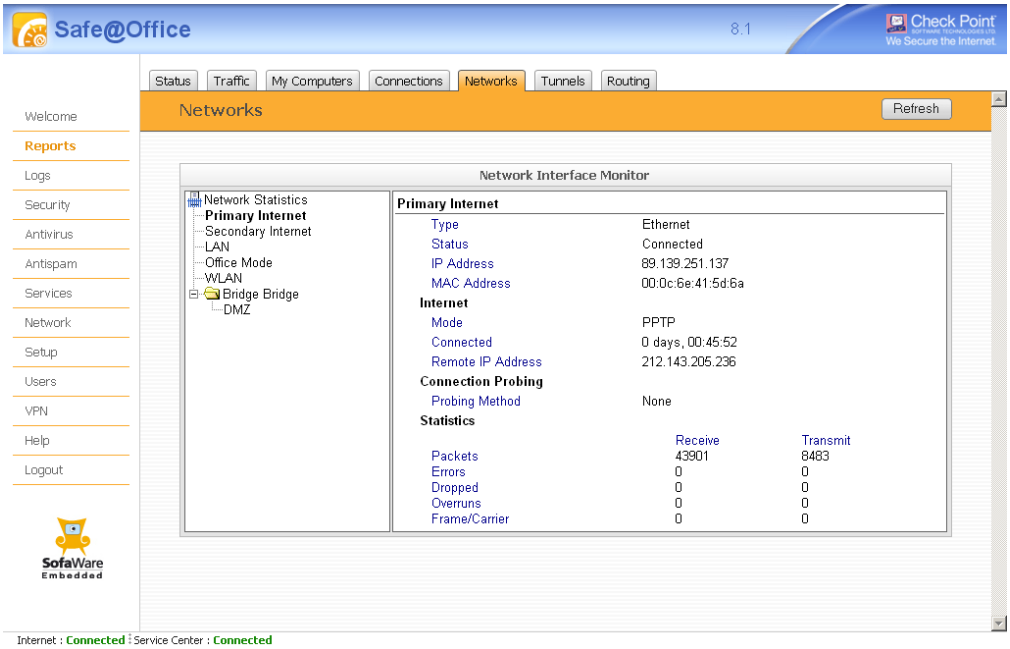
To view statistics for an Internet connection

1. Click Reports in the main menu, and click the Networks tab.

   The Networks page appears.

2. In the tree, click on the Internet connection.

The page displays statistics for the Internet connection. The following example shows statistics for the primary Internet connection.



For information on the fields, see the following table.

3. To refresh the display, click Refresh.

Table 61: Internet Connection Statistics

This field...	Displays...
Type	The Internet connection's type
Status	The Internet connection's status
IP Address	The appliance's current IP address on the network interface
MAC Address	The appliance's MAC address on the network interface

This field...	Displays...
Internet	
Mode	The Internet connection method used
Connected	The connection duration, in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds
Remote IP Address	The IP address of the PPP peer. This field is only relevant for PPP-based Internet connections.
Connection Probing	
Probing Method	The connection probing method configured for the Internet connection
ADSL	These fields only appear for ADSL connections.
Standard	The DSL line's standard
Annex	The Safe@Office ADSL model (Annex A, Annex B)
Self Test	Indicates whether DSL modem has passed a self-test
Trellis Coding	The DSL line's trellis coding
Framing Structure	The DSL line's framing structure
Line Rate	The line rate for transmission (TX) and reception (RX) in kbps
ADSL Firmware	The installed ADSL firmware
ADSL Firmware [Backup]	The installed backup ADSL firmware

This field...	Displays...
RF status	These fields only appear for ADSL connections.
Tx Power	The local and remote transmission power in dB
SNR Margin	The local and remote Signal to Noise Ration (SNR) margin in dB. The SNR margin is the difference between the amount of noise received by the local/remote line end, and the amount of noise it can tolerate.
Line Attenuation	The local and remote line attenuation in dB. The line attenuation is the difference between the signal power transmitted to the local/remote line end, and that which it received.
Modem	These fields only appear if a cellular modem is connected.
Manufacturer	The modem manufacturer
Model	The modem model
Revision	The modem revision
Serial	The modem serial number
Operator	The cellular operator
Signal Strength	The current signal strength in dB
BER	The bit error rate
Access Technology	The access technology used
Statistics	Statistics only appear if the Internet connection is connected
Packets	The total number of transmitted and received packets

This field...	Displays...
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing Wired Network Statistics

500 1000N

You can view statistics for wired network interfaces, including the LAN, DMZ, OfficeMode, tag-based VLANs, and port-based VLANs.

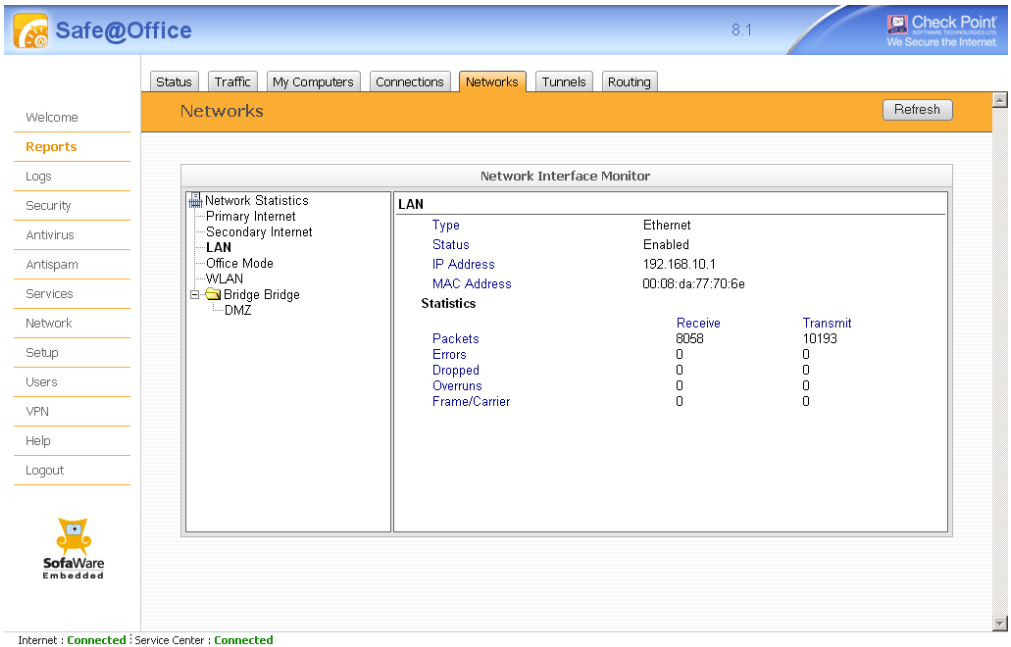
To view statistics for a wired network

1. Click Reports in the main menu, and click the Networks tab.

   The Networks page appears.

2. In the tree, click on the wired network.

   The page displays statistics for the network. The following example shows statistics for the LAN. For information on the fields, see the following table.



3. To refresh the display, click Refresh.

Table 62: Wired Network Statistics

This field…	Displays…
Type	The network's type.
Status	The network's current status (Enabled/Disabled).
IP Address	The appliance's current IP address on the network interface.
MAC Address	The appliance's MAC address on the network interface.
Statistics	Statistics only appear if the network is enabled
Packets	The total number of transmitted and received packets
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing Wireless Network Statistics

500W 1000NW

If the primary WLAN is enabled, you can view wireless statistics for the primary WLAN and VAPs.

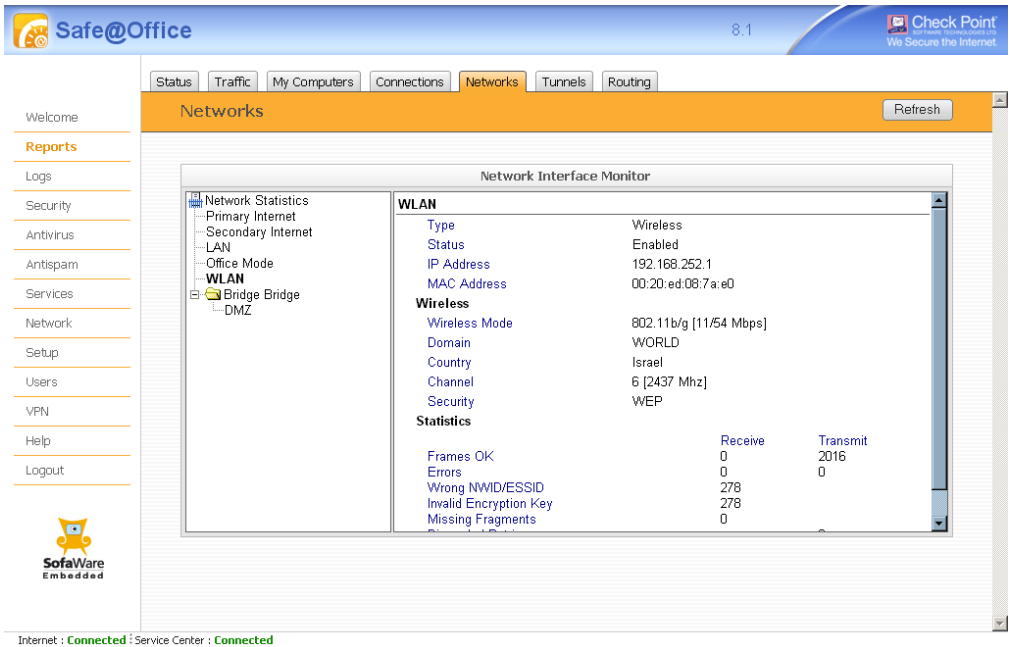
To view statistics for the primary WLAN and VAPs

1. Click Reports in the main menu, and click the Networks tab.

   The Networks page appears.

2. In the tree, click on the wireless network's name.

   The page displays statistics for the network. For information on the fields, see the following table.



3. To refresh the display, click Refresh.

Table 63: Wireless Statistics

This field…	Displays…
Type	The network's type, in this case "Wireless"
Status	The network's current status (Enabled/Disabled)
IP Address	The IP address of the wireless network's default gateway
MAC Address	The MAC address of the wireless network interface
Wireless	
Wireless Mode	The operation mode used by the WLAN, followed by the transmission rate in Mbps
Domain	The Safe@Office access point's region
Country	The country configured for the WLAN
Channel	The radio frequency used by the WLAN
Security	The security mode used by the wireless network
Statistics	Statistics only appear if the network is enabled
Frames OK	The total number of frames that were successfully transmitted and received
Errors	The total number of transmitted and received frames for which an error occurred
Wrong NWID/ESSID	The total number of received packets that were dropped, because they were destined for another access point
Invalid Encryption Key	The total number of transmitted and received packets with the wrong encryption key

This field...	Displays...
Missing Fragments	The total number of packets missed during transmission and reception that were dropped, because fragments of the packet were lost
Discarded Retries	The total number of discarded retry packets that were transmitted and received
Discarded Misc	The total number of transmitted and received packets that were discarded for other reasons

Viewing Bridge Statistics

You can view statistics for bridges.

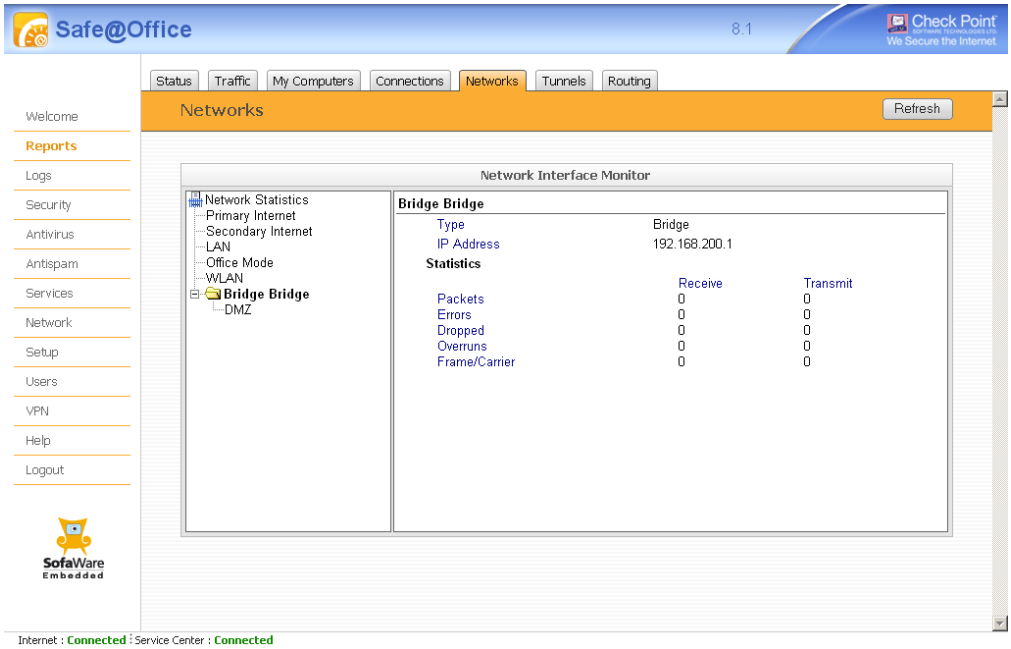
To view statistics for a bridge

1. Click Reports in the main menu, and click the Networks tab.

   The Networks page appears.

2. In the tree, click on the bridge.

The page displays statistics for the bridge. For information on the fields, see the following table.



3. To view statistics for bridged networks, in the tree, expand the bridge's node.

   The page displays statistics for the bridged network.

4. To refresh the display, click Refresh.

Table 64: Bridge Statistics

This field...	Displays...
Type	The network's type, in this case "Bridge"
IP Address	The appliance's current IP address on the bridge interface
Statistics	Statistics only appear if the bridge is enabled
Packets	The total number of transmitted and received packets

This field...	Displays...
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing the Routing Table

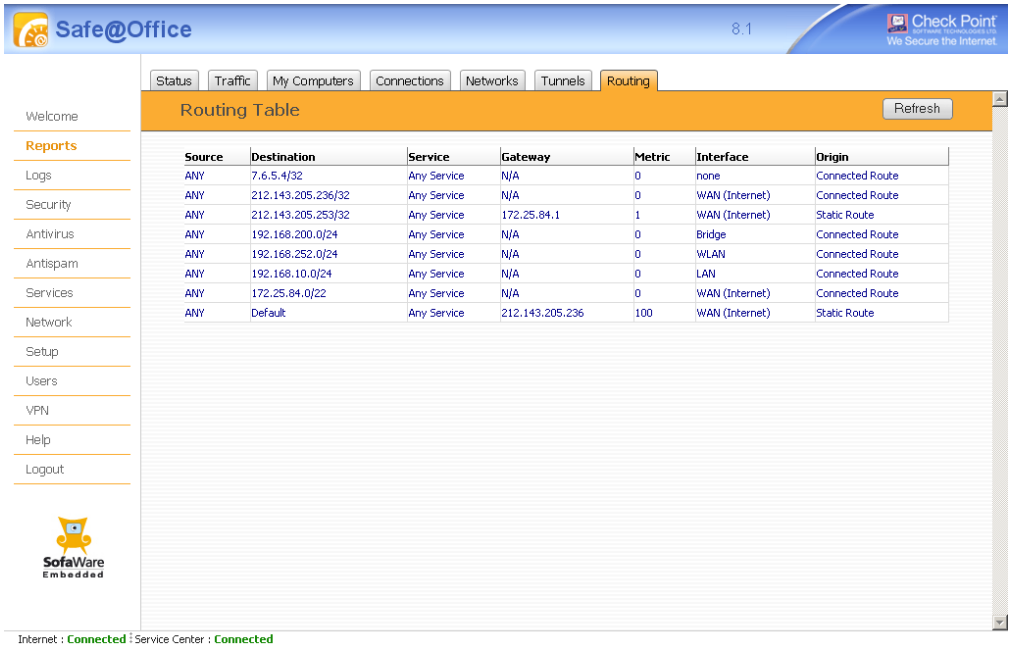
500 1000N

This option allows you to view the routing table currently in effect on the Safe@Office appliance.

To view the current routing table

1. Click Reports in the main menu, and click the Routing tab.

The Routing Table page appears.



The page displays the information in the following table.

2. To resize a column, drag the relevant column divider right or left.
3. To refresh the display, click Refresh.

Table 65: Routing Table Fields

This field...	Displays...
Source	The route's source
Destination	The route's destination
Service	The network service for which the route is configured
Gateway	The gateway's IP address
Metric	The route's metric

This field...	Displays...
Interface	The interface for which the route is configured
Origin	The route's type: • Connected Route. A route to a network that is directly connected to the Safe@Office appliance • Static Route. A destination-based or service-based static route. See ***Using Static Routes*** on page 241. • Dynamic Route. A route obtained through a dynamic routing protocol, such as OSPF • Source Route. A source-based static route. See ***Using Static Routes*** on page 241.

Viewing Wireless Station Statistics

500W 1000NW

If the primary WLAN is enabled, you can view wireless statistics for individual wireless stations.

To view statistics for a wireless station

1. Click Reports in the main menu, and click the My Computers tab.

   The Active Computers page appears.

   The following information appears next to each wireless station:

   - The signal strength in dB
   - A series of bars representing the signal strength
2. Mouse-over the information icon next to the wireless station.

   A tooltip displays statistics for the wireless station, as described in the following table.
3. To refresh the display, click Refresh.

Table 66: Wireless Station Statistics

This field…	Displays…
Current Rate	The current reception and transmission rate in Mbps
Frames OK	The total number of frames that were successfully transmitted and received
Management	The total number of transmitted and received management packets
Control	The total number of received control packets
Errors	The total number of transmitted and received frames for which an error occurred
Dup ratio	The percentage of frames received more than once.
Cipher	The security protocol used for the wireless connection
QoS	Indicates whether the client is using Multimedia QoS (WMM). Possible values are: • yes. The client is using WMM. • no. The client is not using WMM.
XR	Indicates whether the wireless client supports Extended Range (XR) mode. Possible values are: • yes. The wireless client supports XR mode. • no. The wireless client does not support XR mode.

Chapter 12

Viewing Logs

This chapter describes the Safe@Office appliance logs.

This chapter includes the following topics:

Viewing the Event Log.....379
Viewing the Security Log.....383

Viewing the Event Log

500 1000N

The Event Log displays general appliance events, including the following:

- Authentication attempts
- Changes in setup
- Internet connection status changes
- Errors
- Warnings

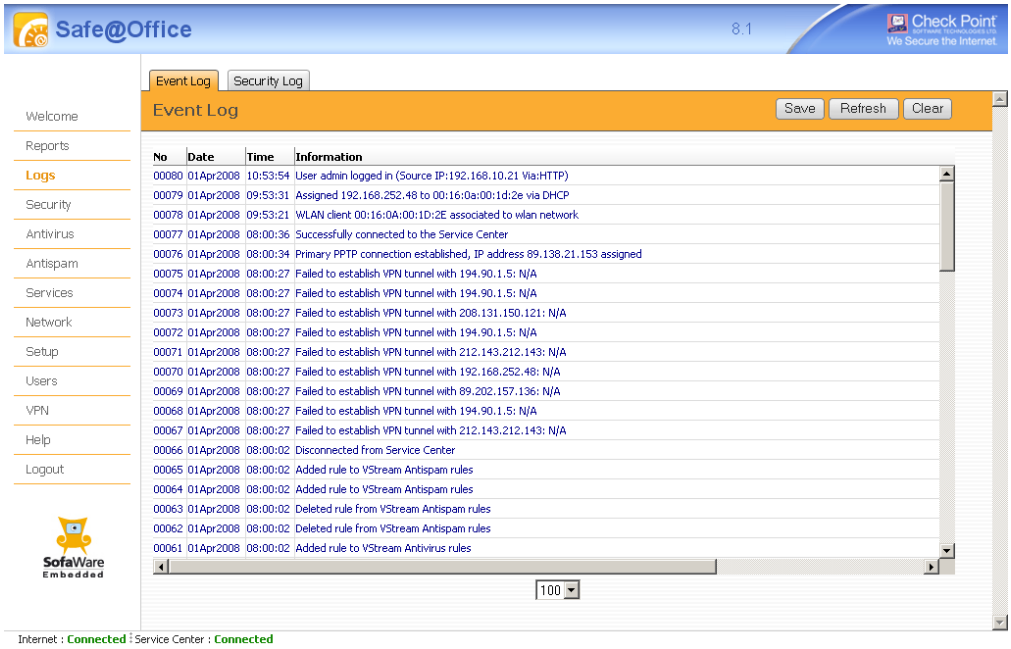
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the Safe@Office appliance to send event and security logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page *726*.

To view the event log

1. Click Logs in the main menu, and click the Event Log tab.

   The Event Log page appears.


Safe@Office
8.1
Check Point
We Secure the Internet.
Event Log
Security Log
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare Embedded
Event Log
Save
Refresh
Clear
No Date Time Information
00080 01Apr2008 10:53:54 User admin logged in (Source IP:192.168.10.21 Via:HTTP)
00079 01Apr2008 09:53:31 Assigned 192.168.252.48 to 00:16:0a:00:1d:2e via DHCP
00078 01Apr2008 09:53:21 WLAN client 00:16:0A:00:1D:2E associated to wlan network
00077 01Apr2008 08:00:36 Successfully connected to the Service Center
00076 01Apr2008 08:00:34 Primary PPTP connection established, IP address 89.138.21.153 assigned
00075 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00074 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00073 01Apr2008 08:00:27 Failed to establish VPN tunnel with 208.131.150.121: N/A
00072 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00071 01Apr2008 08:00:27 Failed to establish VPN tunnel with 212.143.212.143: N/A
00070 01Apr2008 08:00:27 Failed to establish VPN tunnel with 192.168.252.48: N/A
00069 01Apr2008 08:00:27 Failed to establish VPN tunnel with 89.202.157.136: N/A
00068 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00067 01Apr2008 08:00:27 Failed to establish VPN tunnel with 212.143.212.143: N/A
00066 01Apr2008 08:00:02 Disconnected from Service Center
00065 01Apr2008 08:00:02 Added rule to VStream Antispam rules
00064 01Apr2008 08:00:02 Added rule to VStream Antispam rules
00063 01Apr2008 08:00:02 Deleted rule from VStream Antispam rules
00062 01Apr2008 08:00:02 Deleted rule from VStream Antispam rules
00061 01Apr2008 08:00:02 Added rule to VStream Antivirus rules
100
Internet : Connected Service Center : Connected

   The log table contains the columns described in ***Event Log Columns*** on page 382. The log messages are color-coded as described in ***Event Log Color Coding*** on page 383.

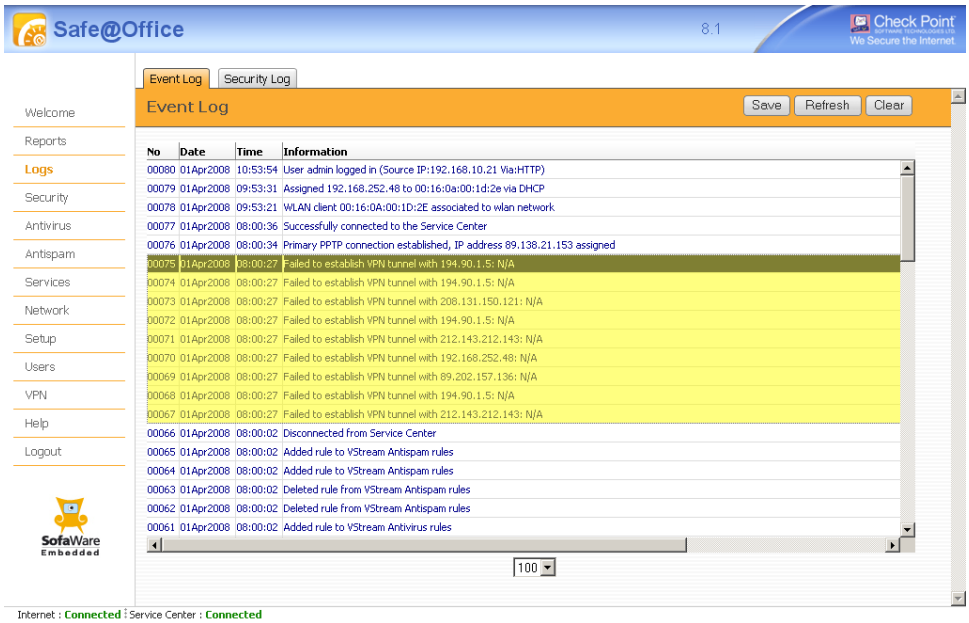
2. To navigate the log table, do any of the following:

   - To scroll through the displayed log page:
     - Use the scroll bars, or
     - Click on a log message and then press the UP and DOWN arrows on your keyboard.
   - To view the next log page, click Next.
   - To view the previous log page, click Back.

3. To specify the number of logs to display per page, in the drop-down list at the bottom of the log table, select the desired number.

4. To resize a column, drag the relevant column divider right or left.

5. To refresh the display, click **Refresh**.
6. To save the displayed events to an *.xls file:
   a. Click **Save**.
      A standard **File Download** dialog box appears.
   b. Click **Save**.
      The **Save As** dialog box appears.
   c. Browse to a destination directory of your choice.
   d. Type a name for the configuration file and click **Save**.
      The *.xls file is created and saved to the specified directory.
7. To copy log messages, do the following:
   a. Select the desired logs, by clicking in the log table and dragging the cursor.
      The selected logs are highlighted in yellow.


Safe@Office
8.1
Check Point
We Secure the Internet.
Event Log
Security Log
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare Embedded
Event Log
Save
Refresh
Clear
No Date Time Information
00080 01Apr2008 10:53:54 User admin logged in (Source IP:192.168.10.21 Via:HTTP)
00079 01Apr2008 09:53:31 Assigned 192.168.252.48 to 00:16:0a:00:1d:2e via DHCP
00078 01Apr2008 09:53:21 WLAN client 00:16:0A:00:1D:2E associated to wlan network
00077 01Apr2008 08:00:36 Successfully connected to the Service Center
00076 01Apr2008 08:00:34 Primary PPTP connection established, IP address 89.138.21.153 assigned
00075 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00074 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00073 01Apr2008 08:00:27 Failed to establish VPN tunnel with 208.131.150.121: N/A
00072 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00071 01Apr2008 08:00:27 Failed to establish VPN tunnel with 212.143.212.143: N/A
00070 01Apr2008 08:00:27 Failed to establish VPN tunnel with 192.168.252.48: N/A
00069 01Apr2008 08:00:27 Failed to establish VPN tunnel with 89.202.157.136: N/A
00068 01Apr2008 08:00:27 Failed to establish VPN tunnel with 194.90.1.5: N/A
00067 01Apr2008 08:00:27 Failed to establish VPN tunnel with 212.143.212.143: N/A
00066 01Apr2008 08:00:02 Disconnected from Service Center
00065 01Apr2008 08:00:02 Added rule to VStream Antispam rules
00064 01Apr2008 08:00:02 Added rule to VStream Antispam rules
00063 01Apr2008 08:00:02 Deleted rule from VStream Antispam rules
00062 01Apr2008 08:00:02 Deleted rule from VStream Antispam rules
00061 01Apr2008 08:00:02 Added rule to VStream Antivirus rules
100
Internet : Connected Service Center : Connected

   b. Press CTRL+C.

If you are using Internet Explorer, and this is the first time that you copy logs, a dialog box asks you whether you want to allow the Safe@Office Portal to access your clipboard. In this case, click Allow access.

The selected logs are copied to your clipboard.

8. To clear all displayed events:
   a. Click Clear.
      A confirmation message appears.
   b. Click OK.
      All events are cleared.

Table 67: Event Log Columns

This column...	Displays...
No	The log message number
Date	The date on which the event occurred, in the format DD:MM:YYYY, where: DD=date MM=month, in abbreviated form YYYY=year
Time	The time at which the event occurred, in the format hh:mm:ss, where: hh=hour mm=minutes ss=seconds
Information	A description of the logged event

Table 68: Event Log Color Coding

An event marked in this color…	Indicates…
Red	An error message
Orange	A warning message
Blue	An informational message

Viewing the Security Log

500 1000N

The Security Log displays security-related events, including the following:

- Connections logged by firewall rules
- Connections logged by VStream Antivirus
- Connection logged by VStream Antispam
- Security events logged by SmartDefense
- Web sites blocked by Web rules or the centralized Web Filtering service

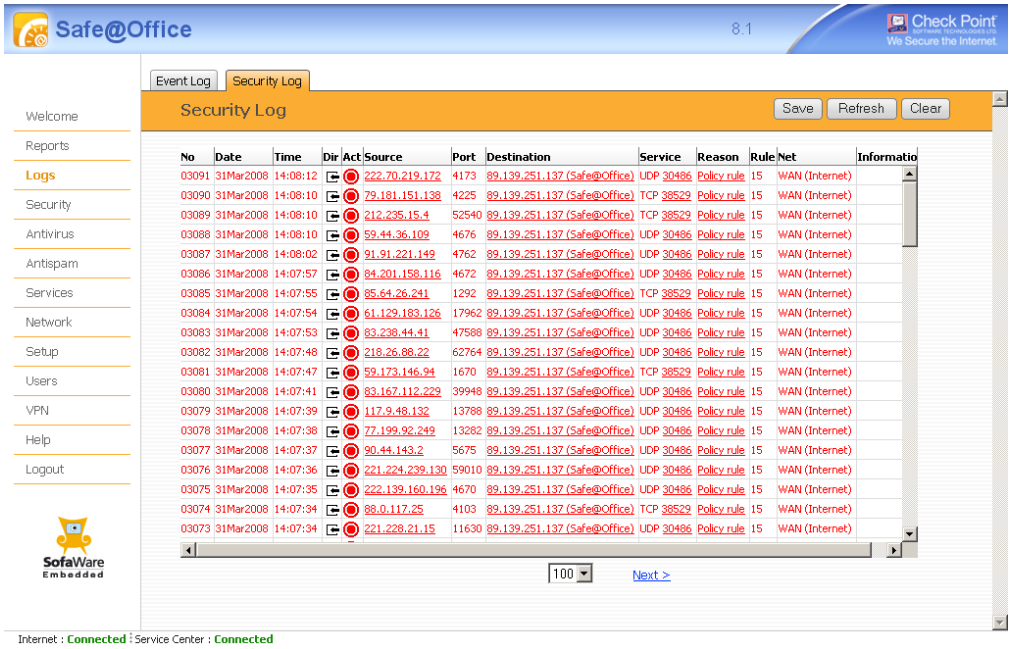
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the Safe@Office appliance to send event and security logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page *726*.

To view the security log

1. Click Logs in the main menu, and click the Security Log tab.

   The Security Log page appears.


Safe@Office
8.1
Check Point
We Secure the Internet
Event Log
Security Log
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare Embedded
Security Log
Save
Refresh
Clear
No Date Time Dir Act Source Port Destination Service Reason Rule Net Informatio
03091 31Mar2008 14:08:12 222.70.219.172 4173 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03090 31Mar2008 14:08:10 79.181.151.138 4225 89.139.251.137 (Safe@Office) TCP 38529 Policy rule 15 WAN (Internet)
03089 31Mar2008 14:08:10 212.235.15.4 52540 89.139.251.137 (Safe@Office) TCP 38529 Policy rule 15 WAN (Internet)
03088 31Mar2008 14:08:10 59.44.36.109 4676 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03087 31Mar2008 14:08:02 91.91.221.149 4762 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03086 31Mar2008 14:07:57 84.201.158.116 4672 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03085 31Mar2008 14:07:55 85.64.26.241 1292 89.139.251.137 (Safe@Office) TCP 38529 Policy rule 15 WAN (Internet)
03084 31Mar2008 14:07:54 61.129.183.126 17962 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03083 31Mar2008 14:07:53 83.238.44.41 47588 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03082 31Mar2008 14:07:48 218.26.88.22 62764 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03081 31Mar2008 14:07:47 59.173.146.94 1670 89.139.251.137 (Safe@Office) TCP 38529 Policy rule 15 WAN (Internet)
03080 31Mar2008 14:07:41 83.167.112.229 39948 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03079 31Mar2008 14:07:39 117.9.48.132 13788 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03078 31Mar2008 14:07:38 77.199.92.249 13282 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03077 31Mar2008 14:07:37 90.44.143.2 5675 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03076 31Mar2008 14:07:36 221.224.239.130 59010 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03075 31Mar2008 14:07:35 222.139.160.196 4670 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
03074 31Mar2008 14:07:34 88.0.117.25 4103 89.139.251.137 (Safe@Office) TCP 38529 Policy rule 15 WAN (Internet)
03073 31Mar2008 14:07:34 221.228.21.15 11630 89.139.251.137 (Safe@Office) UDP 30486 Policy rule 15 WAN (Internet)
100
Next >
Internet : Connected Service Center : Connected

   The log table contains the columns described in ***Security Log Columns*** on page 387. The log messages are color-coded as described in ***Security Log Color Coding*** on page 389.

2. To display information about a connection source or destination, click the relevant IP address.

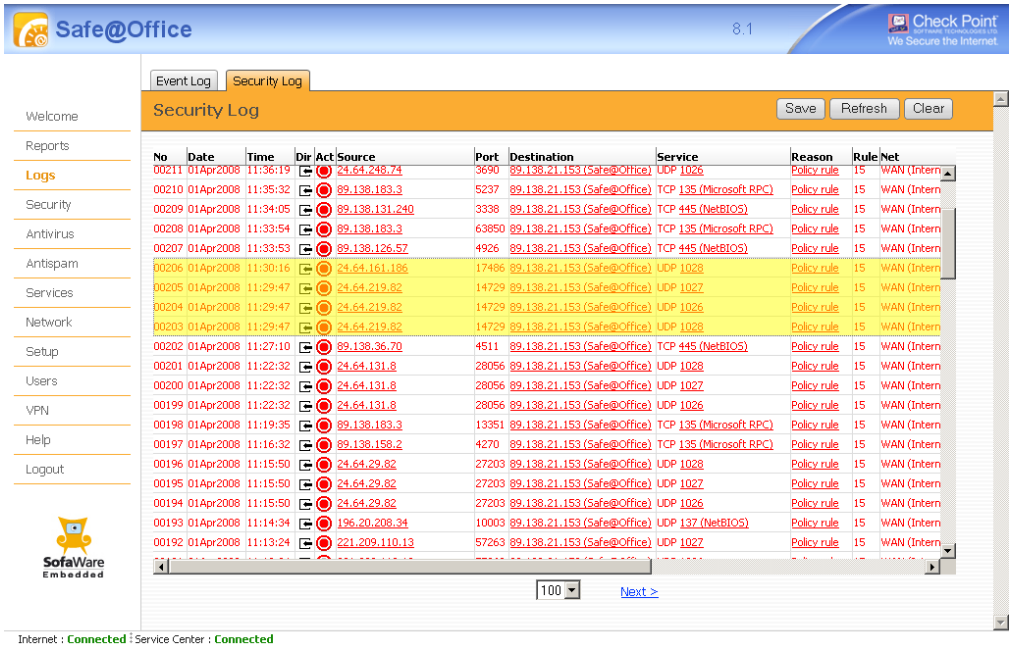
   The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information. This information is useful in tracking down hackers.

3. To view information about a destination port, click the port.

   A window opens displaying information about the port.

4. To navigate the log table, do any of the following:
   - To scroll through the displayed log page:
     - Use the scroll bars, or
     - Click on a log message and then press the UP and DOWN arrows on your keyboard.
   - To view the next log page, click Next.
   - To view the previous log page, click Back.
5. To specify the number of logs to display per page, in the drop-down list at the bottom of the log table, select the desired number.
6. To resize a column, drag the relevant column divider right or left.
7. To refresh the display, click Refresh.
8. To save the displayed events to an *.xls file:
   a. Click Save.
      A standard File Download dialog box appears.
   b. Click Save.
      The Save As dialog box appears.
   c. Browse to a destination directory of your choice.
   d. Type a name for the configuration file and click Save.
      The *.xls file is created and saved to the specified directory.
9. To copy log messages, do the following:
   a. Select the desired logs, by clicking in the log table and dragging the cursor.

The selected logs are highlighted in yellow.


Safe@Office
8.1
Check Point
We Secure the Internet.
Event Log
Security Log
Security Log
Save
Refresh
Clear
Welcome
Reports
Logs
Security
Antivirus
Antispam
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare
Embedded
No Date Time Dir Act Source Port Destination Service Reason Rule Net
00211 01Apr2008 11:36:19 24.64.248.74 3690 89.138.21.153 (Safe@Office) UDP 1026 Policy rule 15 WAN (Intern
00210 01Apr2008 11:35:32 89.138.183.3 5237 89.138.21.153 (Safe@Office) TCP 135 (Microsoft RPC) Policy rule 15 WAN (Intern
00209 01Apr2008 11:34:05 89.138.131.240 3338 89.138.21.153 (Safe@Office) TCP 445 (NetBIOS) Policy rule 15 WAN (Intern
00208 01Apr2008 11:33:54 89.138.183.3 63850 89.138.21.153 (Safe@Office) TCP 135 (Microsoft RPC) Policy rule 15 WAN (Intern
00207 01Apr2008 11:33:53 89.138.126.57 4926 89.138.21.153 (Safe@Office) TCP 445 (NetBIOS) Policy rule 15 WAN (Intern
00206 01Apr2008 11:30:16 24.64.161.186 17486 89.138.21.153 (Safe@Office) UDP 1028 Policy rule 15 WAN (Intern
00205 01Apr2008 11:29:47 24.64.219.82 14729 89.138.21.153 (Safe@Office) UDP 1027 Policy rule 15 WAN (Intern
00204 01Apr2008 11:29:47 24.64.219.82 14729 89.138.21.153 (Safe@Office) UDP 1026 Policy rule 15 WAN (Intern
00203 01Apr2008 11:29:47 24.64.219.82 14729 89.138.21.153 (Safe@Office) UDP 1028 Policy rule 15 WAN (Intern
00202 01Apr2008 11:27:10 89.138.36.70 4511 89.138.21.153 (Safe@Office) TCP 445 (NetBIOS) Policy rule 15 WAN (Intern
00201 01Apr2008 11:22:32 24.64.131.8 28056 89.138.21.153 (Safe@Office) UDP 1028 Policy rule 15 WAN (Intern
00200 01Apr2008 11:22:32 24.64.131.8 28056 89.138.21.153 (Safe@Office) UDP 1027 Policy rule 15 WAN (Intern
00199 01Apr2008 11:22:32 24.64.131.8 28056 89.138.21.153 (Safe@Office) UDP 1026 Policy rule 15 WAN (Intern
00198 01Apr2008 11:19:35 89.138.183.3 13351 89.138.21.153 (Safe@Office) TCP 135 (Microsoft RPC) Policy rule 15 WAN (Intern
00197 01Apr2008 11:16:32 89.138.158.2 4270 89.138.21.153 (Safe@Office) TCP 135 (Microsoft RPC) Policy rule 15 WAN (Intern
00196 01Apr2008 11:15:50 24.64.29.82 27203 89.138.21.153 (Safe@Office) UDP 1028 Policy rule 15 WAN (Intern
00195 01Apr2008 11:15:50 24.64.29.82 27203 89.138.21.153 (Safe@Office) UDP 1027 Policy rule 15 WAN (Intern
00194 01Apr2008 11:15:50 24.64.29.82 27203 89.138.21.153 (Safe@Office) UDP 1026 Policy rule 15 WAN (Intern
00193 01Apr2008 11:14:34 196.20.208.34 10003 89.138.21.153 (Safe@Office) UDP 137 (NetBIOS) Policy rule 15 WAN (Intern
00192 01Apr2008 11:13:24 221.209.110.13 57263 89.138.21.153 (Safe@Office) UDP 1027 Policy rule 15 WAN (Intern
100
Next >
Internet : Connected
Service Center : Connected

b. Press CTRL+C.

   If you are using Internet Explorer, and this is the first time that you copy logs, a dialog box asks you whether you want to allow the Safe@Office Portal to access your clipboard. In this case, click Allow access.

   The selected logs are copied to your clipboard.

10. To clear all displayed events:

    a. Click Clear.

       A confirmation message appears.

    b. Click OK.

       All events are cleared.

Table 69: Security Log Columns

This column...	Displays...
No	The log message number
Date	The date on which the action occurred, in the format DD:MM:YYYY, where: DD=date MM=month, in abbreviated form YYYY=year
Time	The time at which the action occurred, in the format hh:mm:ss, where: hh=hour mm=minutes ss=seconds
Dir	An icon indicating the direction of the connection on which the firewall acted. This can be one of the following: • Incoming connection • Outgoing connection • Internal connection
Act	An icon indicating the action that the firewall performed on a connection. For a list of Actions icons, see ***Security Log Actions*** on page 388.
Source	The IP address of the connection's source.
Port	The source port used for the connection.
Destination	The IP address of the connection's destination.

This column...	Displays...
Service	The protocol and destination port used for the connection.
Reason	The reason the action was logged.
Rule	The number of the firewall rule that was executed.
Net	The internal network where the action occurred.
Information	Additional information about the logged action.

Table 70: Security Log Actions

Action	Icon	Description
Connection Accepted		The firewall accepted a connection.
Connection Decrypted		The firewall decrypted a connection.
Connection Dropped		The firewall dropped a connection.
Connection Encrypted		The firewall encrypted a connection.
Connection Rejected		The firewall rejected a connection.
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration.
URL Allowed		The firewall allowed a URL.
URL Filtered		The firewall blocked a URL.
Virus Detected		A virus was detected in an email.
Potential Spam Stamped		An email was marked as potential spam.

Action	Icon	Description
Potential Spam Detected		An email was rejected as potential spam.
Mail Allowed		A non-spam email was logged.
Blocked by VStream Antivirus		VStream Antivirus blocked a connection.

Table 71: Security Log Color Coding

An event marked in this color…	Indicates…
Red	Connection attempts that were blocked by your firewall, by a security policy downloaded from your Service Center, or by user-defined rules.
Orange	Traffic detected as suspicious, but accepted by the firewall. For example, if a SmartDefense protection's Action field is set to "Track" instead of "Block", and a connection triggers this protection, the connection is accepted and logged in orange.
Green	Traffic accepted by the firewall. By default, accepted traffic is not logged. However, such traffic may be logged if specified by a security policy downloaded from your Service Center, or if specified in user-defined rules.

Chapter 13

Setting Your Security Policy

This chapter describes how to set up your Safe@Office appliance security policy.

You can enhance your security policy by subscribing to services such as Web Filtering and Email Filtering. For information on subscribing to services, see ***Using Subscription Services*** on page 591.

This chapter includes the following topics:

The Safe@Office Firewall Security Policy 391
Default Security Policy.....393
Setting the Firewall Security Level 394
Configuring Servers.....397
Using Rules 400
Using Port-Based Security.....413
Using Secure HotSpot 419
Using NAT Rules 425
Using the EAP Authenticator 433

The Safe@Office Firewall Security Policy

What Is a Security Policy?

A security policy is a set of rules that defines your security requirements, including (but not limited to) network security. By themselves, the network security-related rules comprise the network security policy.

When configured with the necessary network security rules, the Safe@Office appliance serves as the enforcement agent for your network security policy. Therefore, the Safe@Office appliance's effectiveness as a security solution is directly related to the network security policy's content.

Security Policy Implementation

The key to implementing a network security policy is to understand that a firewall is simply a technical tool that reflects and enforces a network security policy for accessing network resources.

A *rule base* is an ordered set of individual network security rules, against which each attempted connection is checked. Each rule specifies the source, destination, service, and action to be taken for each connection. A rule also specifies how a communication is tracked, logged, and displayed. In other words, the rule base is the implementation of the security policy.

Security Policy Enforcement

The Safe@Office appliance uses the unique, patented INSPECT engine to enforce the configured security policy and to control traffic between networks. The INSPECT engine examines all communication layers and extracts only the relevant data, enabling highly efficient operation, support for a large number of protocols and applications, and easy extensibility to new applications and services.

Planning the Safe@Office Firewall Security Policy

Before creating a security policy for your system, answer the following questions:

- Which services, including customized services and sessions, are allowed across the network?
- Which user permissions and authentication schemes are needed?
- Which objects are in the network? Examples include gateways, hosts, networks, routers, and domains.
- Which network objects can connect to others, and should the connections be encrypted?
- What should be the event logging policy?
- Which Quality of Service (QoS) classes will you need?

Default Security Policy

The Safe@Office default security policy includes the following rules:

- Access is blocked from the WAN (Internet) to all internal networks (LAN, DMZ, primary WLAN, VLANs, VAPs, and OfficeMode).
- Access is allowed from the internal networks to the WAN, according to the firewall security level (Low/Medium/High).
- Access is allowed from the LAN network to the other internal networks (DMZ, primary WLAN, VLANs, VAPs, and OfficeMode).
- Access is blocked from the DMZ, primary WLAN, VLAN, VAP, and OfficeMode networks to the other internal networks, (including between different VLANs and VAPs).
- HTTPS access to the Safe@Office Portal (my.firewall, my.hotspot, and my.vpn) is allowed from all internal networks.
- HTTP access to the Safe@Office Portal (my.firewall, my.hotspot, and my.vpn) is allowed from all internal networks except the WLAN and VAPs. You can allow HTTP access from the primary WLAN and VAPs by creating a specific user-defined firewall rule.
- When using the print server function (see ***Using Network Printers*** on page 767), access from internal networks to connected network printers is allowed.
- Access from the WAN to network printers is blocked.

These rules are independent of the firewall security level.

You can easily override the default security policy, by creating user-defined firewall rules. For further information, see ***Using Rules*** on page 400.

Setting the Firewall Security Level

500 1000N

The firewall security level can be controlled using a simple lever available on the Firewall page. You can set the lever to the following states.

Table 72: Firewall Security Levels

This level…	Does this…	Further Details
Low	Enforces basic control on incoming connections, while permitting all outgoing connections.	All inbound traffic is blocked to the external Safe@Office appliance IP address, except for ICMP echoes ("pings"). All outbound connections are allowed.
Medium	Enforces strict control on all incoming connections, while permitting safe outgoing connections. This is the default level and is recommended for most cases. Leave it unchanged unless you have a specific need for a higher or lower security level.	All inbound traffic is blocked. All outbound traffic is allowed to the Internet except for Windows file sharing (NBT ports 137, 138, 139 and 445).
High	Enforces strict control on all incoming and outgoing connections.	All inbound traffic is blocked. Restricts all outbound traffic except for the following: Web traffic (HTTP, HTTPS), email (IMAP, POP3, SMTP), ftp, newsgroups, Telnet, DNS, IPSEC IKE and VPN traffic.

This level...	Does this...	Further Details
Block All	Blocks all access between networks.	All inbound and outbound traffic is blocked between the internal networks. This does not affect traffic to and from the gateway itself.

The definitions of firewall security levels provided in this table represent the Safe@Office appliance's default security policy.

You can easily override the default security policy, by creating user-defined firewall rules. For further information, see ***Using Rules*** on page 400.

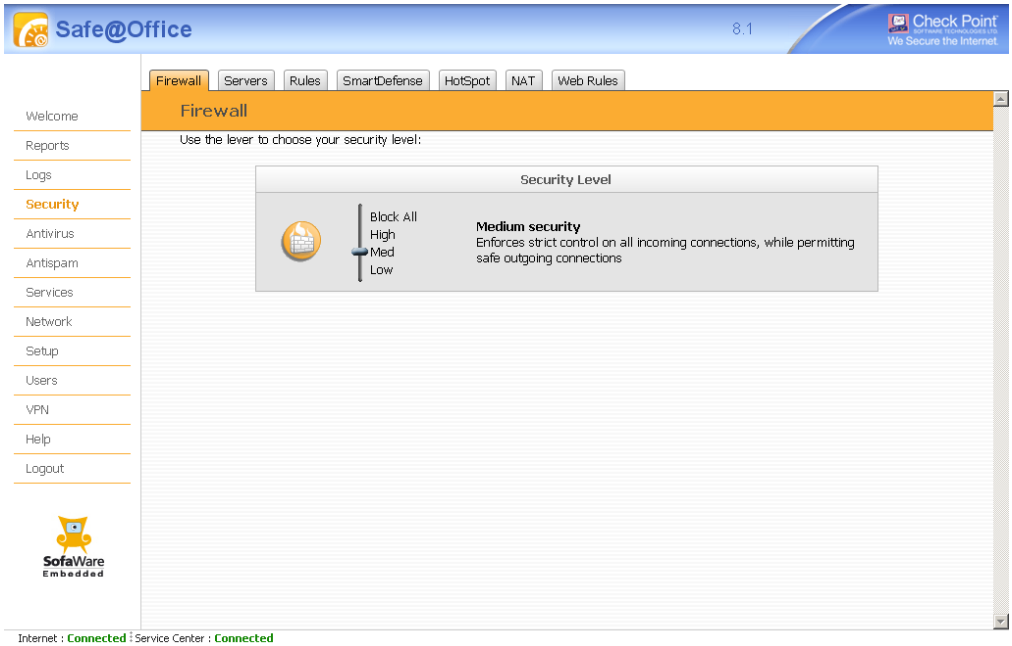
Note: If the security policy is remotely managed, this lever might be disabled.

Note: Security updates downloaded from a Service Center may alter the security policy and change these definitions.

To change the firewall security level

1. Click Security in the main menu, and click the Firewall tab.

The Firewall page appears.



2. Drag the security lever to the desired level.

   The Safe@Office appliance security level changes accordingly.

Configuring Servers

500 1000N

Note: If you do not intend to host any public Internet servers in your network (such as a Web Server, Mail Server, or an exposed host), you can skip this section.

The Safe@Office appliance enables you to configure the following types of public Internet servers:

- Servers for specific services

  You can allow all incoming connections of a specific service and forward them to a particular host in your network. For example, you can set up your own Web server, Mail server, or FTP server.

Note: Configuring servers is equivalent to creating simple Allow and Forward rules for common services, where the destination is This Gateway. For information on creating more complex rules, see ***Using Rules*** on page *400*.

- Exposed host

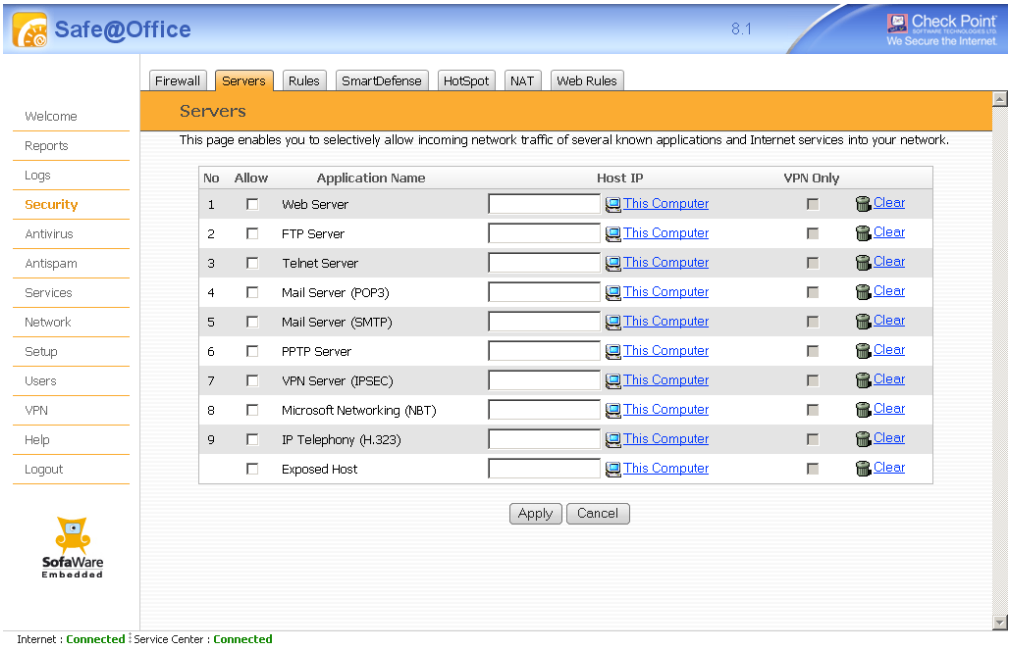
  If you need to allow unlimited incoming and outgoing connections between the Internet and a particular host, you can define an exposed host. An exposed host is not protected by the firewall, and it receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

Warning: Defining an exposed host is not recommended unless you are fully aware of the security risks. For example, an exposed host may be vulnerable to hacker attacks.

To allow services to be run on a specific host

1. Click Security in the main menu, and click the Servers tab.

The Servers page appears, displaying a list of services and a host IP address for each allowed service.



2. Complete the fields using the information in the following table.
3. Click Apply.

   A success message appears.

Table 73: Servers Page Fields

In this column…	Do this…
Allow	Select the check box next to the public server you want to configure. This can be either of the following: • A specific service or application (rows 1-9) • An exposed host (row 10)
Host IP	Type the IP address of the computer that will run the service (one of your network computers), or click the corresponding This Computer button to allow your computer to host the service.
VPN Only	Select this option to allow only connections made through a VPN.

To stop the forwarding of services to a specific host

1. Click Security in the main menu, and click the Servers tab.
   The Servers page appears.
2. In the desired server's row, click Clear.
   The Host IP field is cleared.
3. Click Apply.

Using Rules

500 1000N

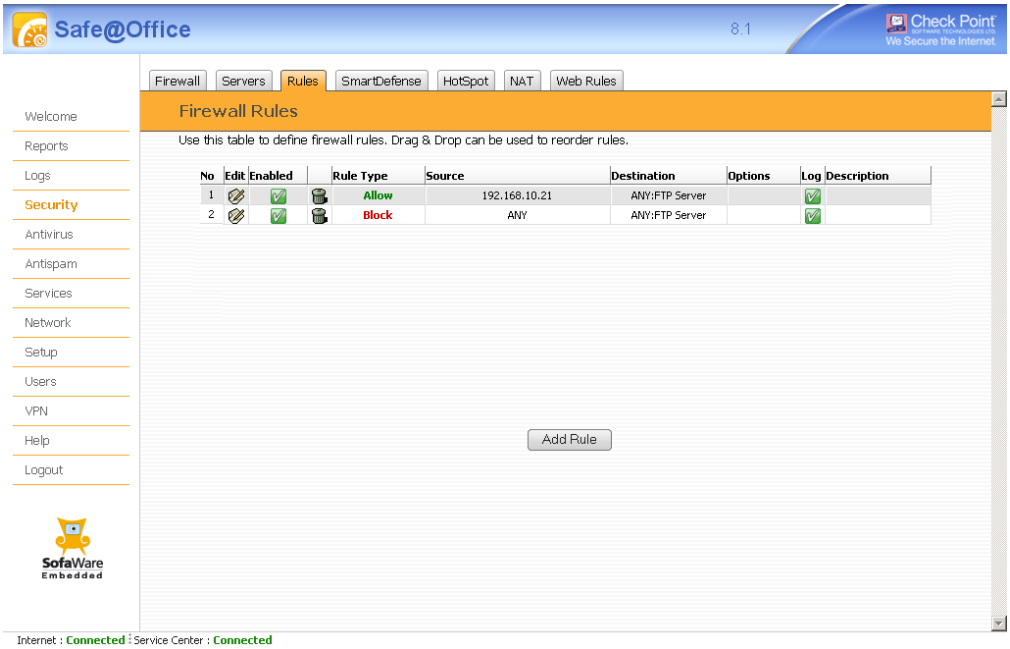
The Safe@Office appliance checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic.

User-defined rules have priority over the default security policy rules and provide you with greater flexibility in defining and customizing your security policy.

For example, if you assign your company's accounting department to the LAN network and the rest of the company to the DMZ network, then as a result of the default security policy rules, the accounting department will be able to connect to all company computers, while the rest of the employees will not be able to access any sensitive information on the accounting department computers. You can override the default security policy rules, by creating firewall rules that allow specific DMZ computers (such a manager's computer) to connect to the LAN network and the accounting department.

The Safe@Office appliance processes user-defined rules in the order they appear in the Rules table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to block all outgoing FTP traffic, except traffic from a specific IP address, you can create a rule blocking all outgoing FTP traffic and move the rule down in the Rules table. Then create a rule allowing FTP traffic from the desired IP address and move this rule to a higher location in the Rules table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The Safe@Office appliance will process rule 1 first, allowing outgoing FTP traffic from the specified IP address, and only then it will process rule 2, blocking all outgoing FTP traffic.

The following rule types exist:

Table 74: Firewall Rule Types

Rule	Description
Allow and Forward	This rule type enables you to do the following: • Permit incoming traffic from the Internet to a specific service and destination IP address in your internal network and then forward all such connections to a specific computer in your network. Such rules are called NAT forwarding rules. For example, if the gateway has two public IP addresses, 62.98.112.1 and 62.98.112.2, and the network contains two private Web servers, A and B, you can forward all traffic with the destination 62.98.112.1 to server A, while forwarding all traffic with the destination 62.98.112.2 to server B. Note: Creating an Allow and Forward rule for incoming traffic to the default destination This Gateway (which represents the Safe@Office IP address), is equivalent to defining a server in the Servers page. • Permit outgoing traffic from your internal network to a specific service and destination IP address on the Internet and then divert all such connections to a specific IP address. Such rules are called transparent proxy rules. For example, you can redirect all traffic destined for a specific Web server on the Internet to a different IP address. • Redirect the specified connections to a specific port. This option is called Port Address Translation (PAT). • Assign traffic to a QoS class. If Traffic Shaper is enabled for incoming traffic, then Traffic Shaper will handle relevant connections as specified in the bandwidth policy for the selected QoS class. For example, if Traffic Shaper is enabled for incoming traffic, and you create an Allow and Forward rule associating all incoming Web traffic with the Urgent QoS class, then Traffic Shaper will handle incoming Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 293. Note: You must use this type of rule to allow incoming connections if your network uses Hide NAT.

Rule	Description
Allow	This rule type enables you to do the following: • Permit outgoing access from your internal network to a specific service on the Internet. Permit incoming access from the Internet to a specific service in your internal network. • Assign traffic to a QoS class. If Traffic Shaper is enabled for the direction of traffic specified in the rule (incoming or outgoing), then Traffic Shaper will handle relevant connections as specified in the bandwidth policy for the selected QoS class. For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing Web traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 293. Note: You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. Use an “Allow and Forward” rule instead. However, you can use Allow rules for static NAT IP addresses.
Block	This rule type enables you to do the following: • Block outgoing access from your internal network to a specific service on the Internet. • Block incoming access from the Internet to a specific service in your internal network. • Block connections between hosts on different internal networks.

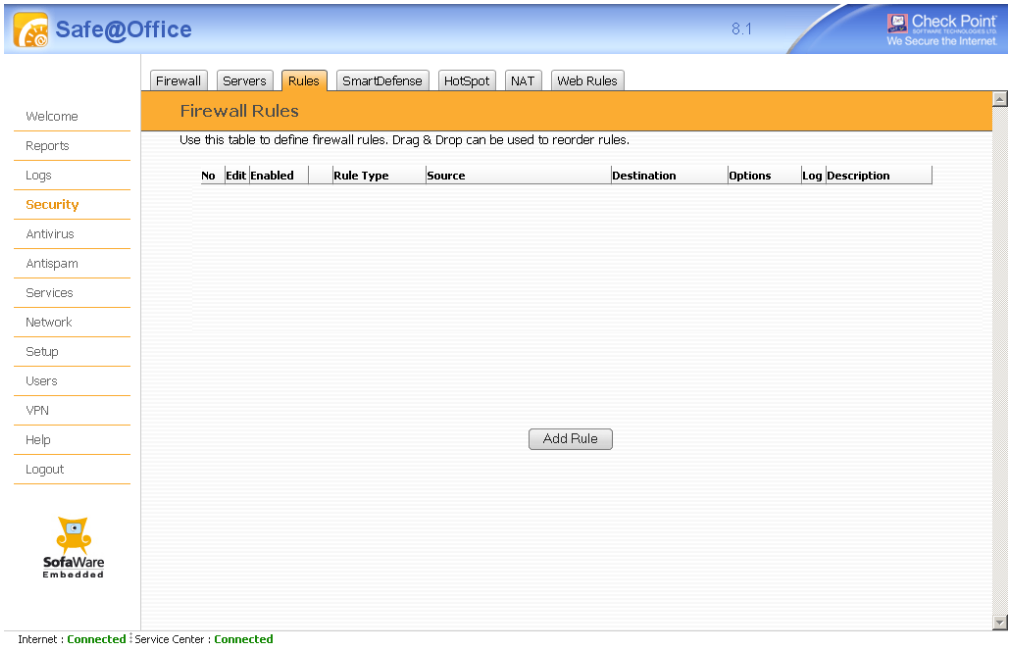
Adding and Editing Firewall Rules

500 1000N

To add or edit a firewall rule

1. Click Security in the main menu, and click the Rules tab.

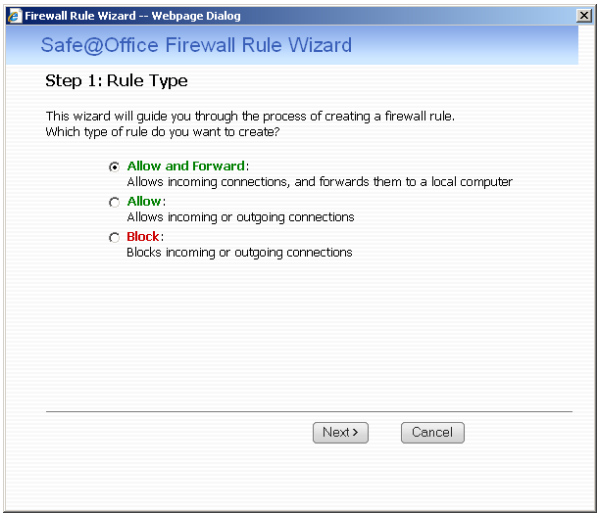
   The Rules page appears.



2. Do one of the following:

   - To add a new rule, click Add Rule.
   - To edit an existing rule, click next to the desired rule.

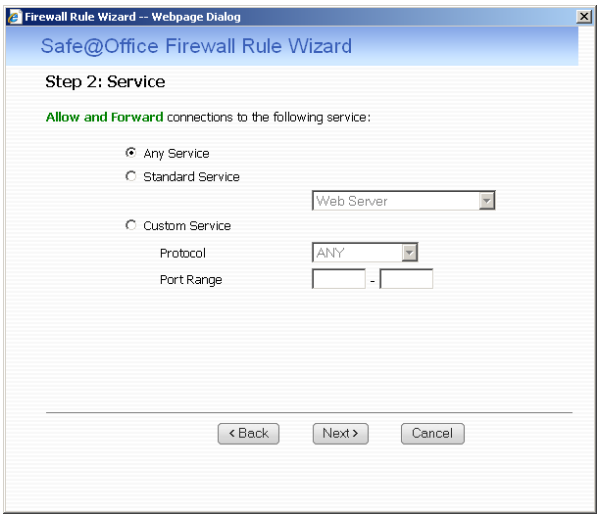
The Safe@Office Firewall Rule wizard opens, with the Step 1: Rule Type dialog box displayed.


Firewall Rule Wizard -- Webpage Dialog
Safe@Office Firewall Rule Wizard
Step 1: Rule Type
This wizard will guide you through the process of creating a firewall rule.
Which type of rule do you want to create?
Allow and Forward:
Allows incoming connections, and forwards them to a local computer
Allow:
Allows incoming or outgoing connections
Block:
Blocks incoming or outgoing connections
Next >
Cancel

3. Select the type of rule you want to create.
4. Click Next.

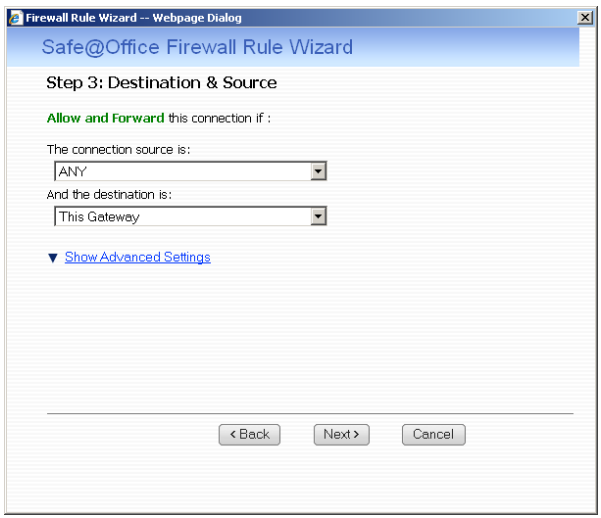
   The Step 2: Service dialog box appears.

   The example below shows an Allow and Forward rule.



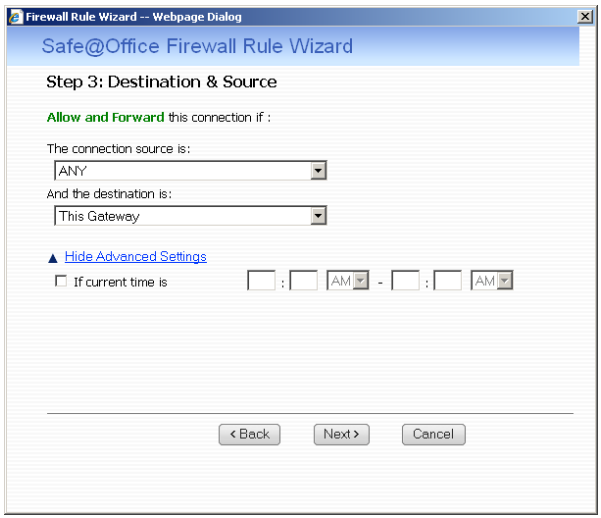
5. Complete the fields using the relevant information in the following table.
6. Click **Next**.

   The **Step 3: Destination & Source** dialog box appears.



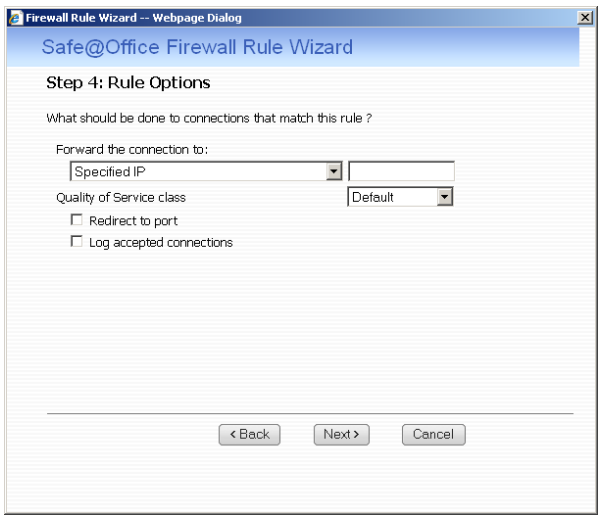
7. To configure advanced settings, click **Show Advanced Settings**.

   New fields appear.



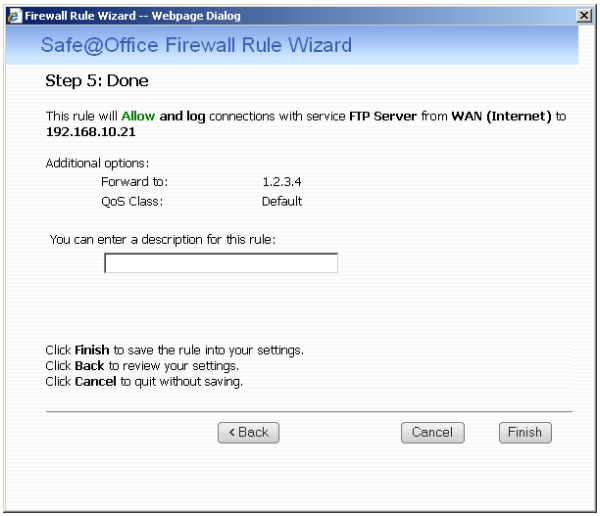
8. Complete the fields using the relevant information in the following table.
9. Click **Next**.

   The **Step 4: Rule Options** dialog box appears.



10. Complete the fields using the relevant information in the following table.
11. Click **Next**.

The Step 5: Done dialog box appears.


Firewall Rule Wizard -- Webpage Dialog
Safe@Office Firewall Rule Wizard
Step 5: Done
This rule will Allow and log connections with service FTP Server from WAN (Internet) to 192.168.10.21
Additional options:
Forward to: 1.2.3.4
QoS Class: Default
You can enter a description for this rule:
Click Finish to save the rule into your settings.
Click Back to review your settings.
Click Cancel to quit without saving.
< Back
Cancel
Finish

12. If desired, type a description of the rule in the field provided.
13. Click Finish.

    The new rule appears in the Rules page.

Table 75: Firewall Rule Fields

In this field...	Do this...
Any Service	Click this option to specify that the rule should apply to any service.
Standard Service	Click this option to specify that the rule should apply to a specific standard service or a network service object. You must then select the desired service or network service object from the drop-down list.
Custom Service	Click this option to specify that the rule should apply to a specific non-standard service. The Protocol and Port Range fields are enabled. You must fill them in.

In this field...	Do this...
Protocol	Select the protocol for which the rule should apply (ESP, GRE, TCP, UDP, ICMP, IGMP, or OSPF). To specify that the rule should apply for any protocol, select ANY. To specify a protocol by number, select Other. The Protocol Number field appears.
Port Range	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. Note: If you do not enter a port range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.
Protocol Number	Type the number of the protocol for which the rule should apply.
Source	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP address, select This Gateway. To specify any source, select ANY.
Destination	Select the destination of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.

In this field...	Do this...
	To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
If the current time is	Select this option to specify that the rule should be applied only during certain hours of the day. You must then use the fields and drop-down lists provided, to specify the desired time range.
Forward the connection to	Select the destination to which matching connections should be forwarded. To specify an IP address, select Specified IP and type the desired IP address in the text box. This field only appears when defining an Allow and Forward rule.
Quality of Service class	Select the QoS class to which you want to assign the specified connections. If Traffic Shaper is enabled, Traffic Shaper will handle these connections as specified in the bandwidth policy for the selected QoS class. If Traffic Shaper is not enabled, this setting is ignored. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 293. This drop-down list only appears when defining an Allow rule or an Allow and Forward rule.
Redirect to port	Select this option to redirect the connections to a specific port. You must then type the desired port in the field provided. This option is called Port Address Translation (PAT), and is only available when defining an Allow and Forward rule.

In this field...	Do this...
Log accepted connections / Log blocked connections	Select this option to log the specified blocked or allowed connections. By default, accepted connections are not logged, and blocked connections are logged. You can modify this behavior by changing the check box's state.

Enabling/Disabling Firewall Rules

500 1000N

You can temporarily disable a user-defined rule.

To enable/disable a firewall rule

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. Next to the desired rule, in the Enabled column, do one of the following:

   - To enable the rule, click .

     The button changes to and the rule is enabled.

   - To disable the rule, click .

     The button changes to and the rule is disabled.

Reordering Firewall Rules

500 1000N

To reorder firewall rules

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Enabling/Disabling Firewall Rule Logging

500 1000N

You can enable or disable logging for a firewall rule, by using the information in ***Adding and Editing Firewall Rules*** on page 404, or by using the following shortcut.

To enable/disable logging for a firewall rule

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. Next to the desired rule, in the Log column, do one of the following:

   - To enable logging, click .

     The button changes to and logging is enabled for the rule.

   - To disable logging, click .

     The button changes to and logging is disabled for the rule.

Viewing and Deleting Firewall Rules

500 1000N

To view or delete an existing firewall rule

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears with a list of existing firewall rules.

2. To resize a column, drag the relevant column divider right or left.
3. To delete a rule, do the following.

   a. In the desired rule's row, click .
   A confirmation message appears.

   b. Click OK.
   The rule is deleted.

Using Port-Based Security

500 1000N Power Pack

The Safe@Office appliance supports the IEEE 802.1x standard for secure authentication of users and devices that are directly attached to Safe@Office appliance's LAN and DMZ ports, as well as the wireless LAN. Authentication can be performed either by an external RADIUS server, or by the Safe@Office appliance's built-in EAP authenticator. For information on the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 433.

When an 802.1x security scheme is implemented for a port, users attempting to connect to that port are required to authenticate using their network user name and password. The Safe@Office appliance sends the user's credentials to the configured authentication server, and if authentication succeeds, a connection is established. If the user fails to authenticate, the port is physically isolated from other ports on the gateway.

If desired, you can specify how users should be handled after successful or failed authentication. Users who authenticate successfully on a specific port are assigned to the network with which that port is associated. For example, if the port is assigned to the DMZ

network, all users who authenticate successfully on that port are assigned to the DMZ network.

When using a RADIUS server for authentication, you can assign authenticated users to specific network segments, by configuring dynamic VLAN assignment on the RADIUS server. Upon successful authentication, the RADIUS server sends RADIUS option 81 [Tunnel-Private-Group-ID] to the Safe@Office appliance, indicating to which network segment the user should be assigned. For example, if a member of the Accounting team connects to a network port and attempts to log in, the Safe@Office appliance relays the information to the RADIUS server, which replies with RADIUS option 81 and the value "Accounting". The appliance then assigns the user's port to the Accounting network, granting the user access to all the resources of the Accounting team.

The Safe@Office appliance also enables you to automatically assign users to a "Quarantine" network when authentication fails. All Quarantine network security and network rules will apply to those users. For example, you can create security rules allowing users on the Quarantine network to access the Internet and blocking them from accessing sensitive company resources. You can also configure Traffic Shaper to grant members of the Quarantine network a lower amount of bandwidth than authorized users.

You can choose to exclude specific network objects from 802.1x port-based security enforcement. Excluded network objects will be able to connect to the Safe@Office appliance's ports and access the network without authenticating. For information on excluding network objects from 802.1x port-based security enforcement, see ***Using Network Objects*** on page 227.

Configuring Port-Based Security

500 1000N Power Pack

To configure 802.1x port-based security for a port

1. Do one of the following:
   - To use the Safe@Office EAP authenticator for authenticating clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wired Clients*** on page 435.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.
   - To use a RADIUS server for authenticating clients, do the following:
     1) Configure a RADIUS server.

        See ***Using RADIUS Authentication*** on page 688.
     2) Configure the clients for 802.1x authentication.

        For information, refer to your RADIUS server documentation.
2. To configure dynamic VLAN assignment, do the following:
   a. Add port-based VLAN networks as needed.

      See ***Adding and Editing Port-Based VLANs*** on page 220.
   b. Configure RADIUS option 81 [Tunnel-Private-Group-ID] on the RADIUS server.

      For information, refer to your RADIUS server documentation.

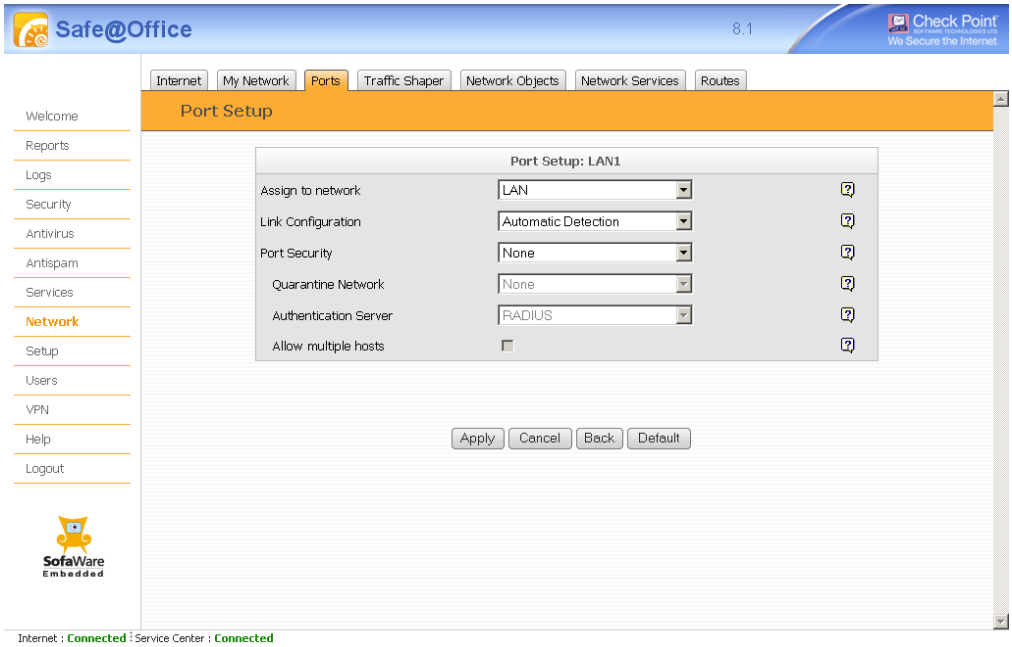
   This step is only relevant when using a RADIUS server.
3. To configure a Quarantine network other than the LAN or DMZ, add a port-based VLAN network.

   See ***Adding and Editing Port-Based VLANs*** on page 220.
4. Click Network in the main menu, and click the Ports tab.

The **Ports** page appears.

5. Next to the desired port, click **Edit**.

The Port Setup page appears.



6. In the Port Security drop-down list, select 802.1x.

   The Quarantine Network, Authentication Server, and Allow multiple hosts fields are enabled.

7. Complete the fields using the information in the following table.

8. Click Apply.

   A warning message appears.

9. Click OK.

Table 76: Port-Based Security Fields

In this field…	Do this…
Assign to network	Specify how the Safe@Office appliance should handle users who authenticate successfully, by selecting one of the following: • A network name. All users who authenticate to this port successfully are assigned to the specified network. • From RADIUS. Use dynamic VLAN assignment to assign users to specific networks. This option is only relevant when using a RADIUS server.
Authentication Server	Specify which authentication server you are using, by selecting one of the following: • RADIUS. A RADIUS server. • Internal User Database. The Safe@Office EAP authenticator.
Quarantine Network	Specify which network should serve as the Quarantine network, by selecting one of the following: • A network name. All users for whom authentication to this port fails are assigned to the specified network. • None. No Quarantine network is selected.
Allow multiple hosts	To allow multiple hosts to connect to this port, select this option. Normally, 802.1x port-based security allows only a single host to connect to each port. However, when this option is selected, multiple clients can connect to the same port via a hub or switch. Each client on the port must authenticate separately. For information on cascading the Safe@Office appliance to a hub or switch, see ***Cascading Your Appliance*** on page 102. Note: Enabling this option makes 802.1x port-based security less secure. Therefore, it is recommended to enable this option only in locations where the number of ports are a limiting factor, and where an external 802.1x-capable switch cannot be installed.

Resetting 802.1x Locking

500 | 1000N | Power Pack

When 802.1x port-based security is configured for a LAN port, the first host that attempts to connect to this port is “locked” to the port. In order to connect a different computer to the port, you must first reset 802.1x locking.

To reset 802.1x locking on all ports

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Click Reset 802.1x.

   A confirmation message appears.

3. Click OK.

   The 802.1x status of all ports is reset to "Unauthenticated".

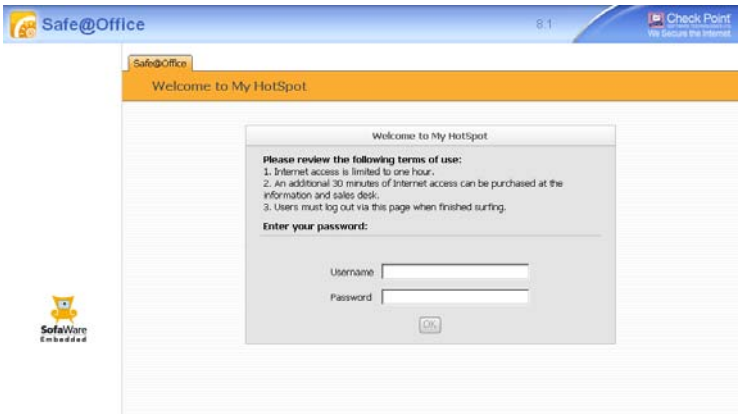
Using Secure HotSpot

Power Pack

You can enable your Safe@Office appliance as a public Internet access hotspot for specific networks. When users on those networks attempt to access the Internet, they are automatically re-directed to the My HotSpot page http://my.hotspot.

Note: You can configure Secure HotSpot to use HTTPS. In this case, the My HotSpot page will be https://my.hotspot.

On this page, users must read and accept the My HotSpot terms of use, and if My HotSpot is configured to be password-protected, they must log in using their Safe@Office username and password. The users may then access the Internet or other corporate networks.


Safe@Office
Check Point
Welcome to My HotSpot
Welcome to My HotSpot
Please review the following terms of use:
1. Internet access is limited to one hour.
2. An additional 30 minutes of Internet access can be purchased at the information and sales desk.
3. Users must log out via this page when finished surfing.
Enter your password:
Username
Password
OK
SofaWare Embedded

Users can also log out in the My HotSpot page.

Note: HotSpot users are automatically logged out after one hour of inactivity. If you are using RADIUS authentication, you can change the Secure HotSpot session timeout by configuring the RADIUS Session-Timeout Attribute. See ***Using RADIUS Authentication*** on page *688*.

Safe@Office Secure HotSpot is useful in any wired or wireless environment where Web-based user authentication or terms-of-use approval is required prior to gaining access to the network. For example, Secure HotSpot can be used in public computer labs, educational institutions, libraries, Internet caf's, and so on. You can also track and charge for Secure HotSpot use, by enabling RADIUS accounting. For information, see ***Using RADIUS Authentication*** on page 688.

The Safe@Office appliance allows you to add guest users quickly and easily. By default, guest users are given a username and password that expire in 24 hours and granted HotSpot Access permissions only. For information on adding quick guest users, see ***Adding Quick Guest Users*** on page 685.

You can choose to exclude specific network objects from HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. Furthermore, users will be able to access the excluded network object without viewing the

My HotSpot page. For information on excluding network objects from HotSpot enforcement, see ***Using Network Objects*** on page 227.

Important: SecuRemote/SecureClient/L2TP/Endpoint Connect VPN software users who are authenticated by the Internal VPN Server are automatically exempt from HotSpot enforcement. This allows, for example, authenticated employees to gain full access to the corporate LAN, while guest users are permitted to access the Internet only.

Note: HotSpot enforcement can block traffic passing through the firewall; however, it does not block local traffic on the same network segment (traffic that does not pass through the firewall).

Setting Up Secure HotSpot

Power Pack

To set up Secure HotSpot

1. Enable Secure HotSpot for the desired networks.

   See ***Enabling/Disabling Secure HotSpot*** on page 422.

2. Customize Secure HotSpot as desired.

   See ***Customizing Secure HotSpot*** on page 423.

3. Grant HotSpot Access permissions to users on the selected networks.

   See ***Adding and Editing Users*** on page 680.

4. To exclude specific computers from Secure HotSpot enforcement, add or edit their network objects.

   See ***Adding and Editing Network Objects*** on page 229.

   You must select Exclude this computer/network from HotSpot enforcement option.

5. Add quick guest users as needed.

   See ***Adding Quick Guest Users*** on page 685.

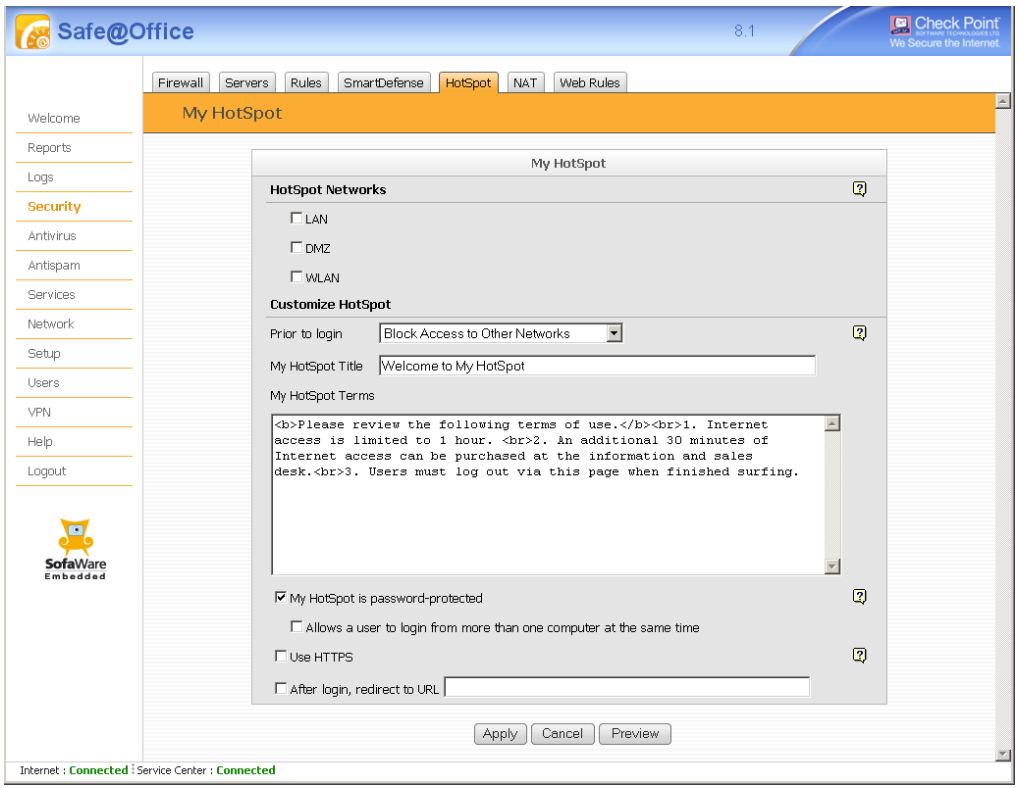
Enabling/Disabling Secure HotSpot

Power Pack

To enable/disable Secure HotSpot

1. Click Security in the main menu, and click the HotSpot tab.

   The My HotSpot page appears.



2. In the HotSpot Networks area, do one of the following:

   - To enable Secure HotSpot for a specific network, select the check box next to the network.
   - To disable Secure HotSpot for a specific network, clear the check box next to the network.

3. Click Apply.

Customizing Secure HotSpot

Power Pack

To customize Secure HotSpot

1. Click Security in the main menu, and click the HotSpot tab.

   The My HotSpot page appears.
2. Complete the fields using the information in the following table.
3. To preview the My HotSpot page, click Preview.

   A browser window opens displaying the My HotSpot page.
4. Click Apply.

   Your changes are saved.

Table 77: My HotSpot Fields

In this field…	Do this…
Prior to login	Specify the degree of access to grant users who have not yet logged in to Secure HotSpot or for whom authentication failed, by selecting one of the following: • Block Access to Other Networks. Users cannot access internal networks, the Internet, or VPN. This is the default. • Block Access to External Networks Only. Users can access internal networks, but not the Internet or VPN. • Block Access to VPN Only. Users can access internal networks and the Internet, but not VPN.
My HotSpot Title	Type the title that should appear on the My HotSpot page. The default title is "Welcome to My HotSpot".

In this field…	Do this…
My HotSpot Terms	Type the terms to which the user must agree before accessing the Internet. You can use HTML tags as needed.
My HotSpot is password-protected	Select this option to require users to enter their username and password before accessing the Internet. If this option is not selected, users will be required only to accept the terms of use before accessing the network. The Allow a user to login from more than one computer at the same time check box appears.
Allow a user to login from more than one computer at the same time	Select this option to allow a single user to log in to My HotSpot from multiple computers at the same time.
Use HTTPS	Select this option to use HTTPS for Secure HotSpot.
After login, redirect to URL	To redirect users to a specific URL after logging in to My HotSpot, select this option and type the desired URL in the field provided. For example, you can redirect authenticated users to your company's Web site or a "Welcome" page.

Using NAT Rules

500 1000N

Overview

In an IP network, each computer is assigned a unique IP address that defines both the host and the network. A computer's IP address can be public and Internet-routable, or private and non-routable. Since IPv4, the current version of IP, provides only 32 bits of address space, available public IP addresses are becoming scarce, most having already been assigned. Internet Service Providers will usually allocate only one or a few public IP addresses at a time, and while larger companies may purchase several such addresses for use, purchasing addresses for every computer on the network is usually impossible.

Due to the lack of available public IP addresses, most computers in an organization are assigned private, non-routable IP addresses. Even if more public IP addresses became available, changing the private IP address of every machine in a large network to a public IP address would be an administrative nightmare, being both labor intensive and time consuming. Therefore, organization's computers will most likely remain with private, non-routable IP addresses, even though in most cases they require access to the Internet.

In addition to the issue of arranging Internet access for computers with non-routable IP addresses, IP networks present a security challenge. Since making a network’s internal addresses public knowledge can reveal the topology of the entire network, the network administrator may want to conceal both routable and non-routable IP addresses from outside the organization, or even from other parts of the same organization, in order to enhance security.

The Safe@Office appliance solves both issues through the use of Network Address Translation (NAT) rules. A NAT rule is a setting used to change the source, destination, and/or service of specific connections.

Supported NAT Rule Types

The Safe@Office appliance enables you to define the following types of *custom NAT rules*:

- Static NAT (or One-to-One NAT). Translation of an IP address range to another IP address range of the same size.

  This type of NAT rule allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. This is useful if you want each computer in your private network to have its own Internet IP addresses.

- Hide NAT (or Many-to-One NAT). Translation of an IP address range to a single IP address.

  This type of NAT rule enables you to share a single public Internet IP address among several computers, by "hiding" the private IP addresses of the internal computers behind the Safe@Office appliance's single Internet IP address. For more information on Hide NAT, see ***How Does Hide NAT Work?*** on page 427.

- Few-to-Many NAT. Translation of a smaller IP address range to a larger IP address range.

  When this type of NAT rule is used, static NAT is used to map the IP addresses in the smaller range to the IP addresses at the beginning of the larger range. The remaining IP addresses in the larger range remain unused.

- Many-to-Few NAT. Translation of a larger IP address range to a smaller IP address range.

  When this type of NAT rule is used, static NAT is used to map the IP addresses in the larger range to all but the final IP address in the smaller range. Hide NAT is then used to map all of the remaining IP addresses in the larger range to the final IP address in the smaller range.

- Service-Based NAT. Translation of a connection's original service to a different service.

The Safe@Office appliance also supports *implicitly defined NAT rules*. Such rules are created automatically upon the following events:

- Hide NAT is enabled on an internal network
- An Allow and Forward firewall rule is defined

- Static NAT is configured for a network object (for information, see ***Using Network Objects*** on page 227)
- NAT rules are received from the Service Center

Implicitly defined NAT rules can only be edited or deleted indirectly. For example, in order to remove a NAT rule created when a certain network object was defined, you must modify the relevant network object.

The Address Translation page displays both custom NAT rules and implicitly defined NAT rules, and it allows you to create, edit, and delete custom NAT rules.

How Does Hide NAT Work?

In Hide NAT, traffic to and from the internal networks traverses an enforcement module. When a packet from an internal network passes through the gateway, the source IP address is changed to the hiding IP address, and the source port is changed to a dynamically assigned port that uniquely identifies the connection. The relationship between the dynamically assigned port and the internal IP address is recorded in the gateway's state tables. When reply packets arrive, the enforcement module uses the destination port to determine to which connection the packet belongs, and then adjusts the destination port and IP address accordingly.

Adding and Editing NAT Rules

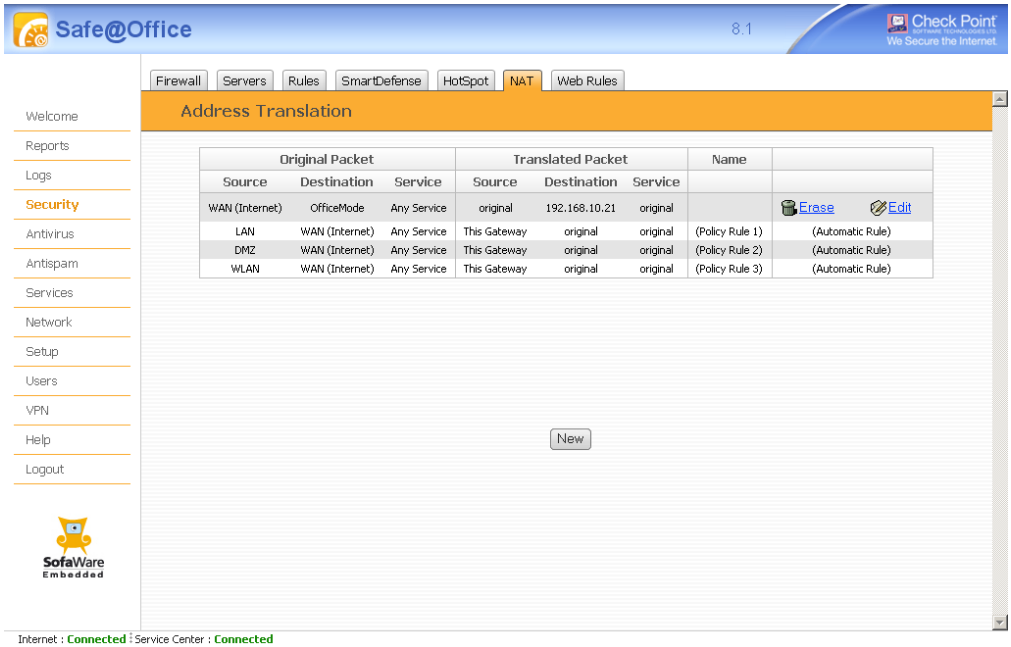
500 1000N

This procedure explains how to add and edit *custom* NAT rules. You cannot add or edit an implicitly defined NAT rule directly.

To add or edit a custom NAT rule

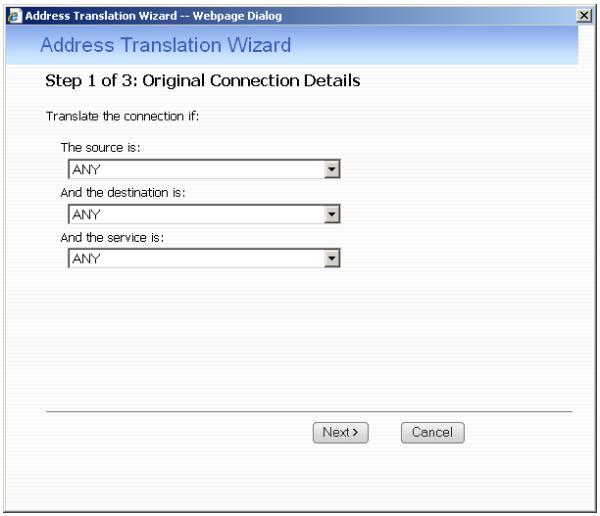
1. Click Security in the main menu, and click the NAT tab.

The Address Translation page appears.



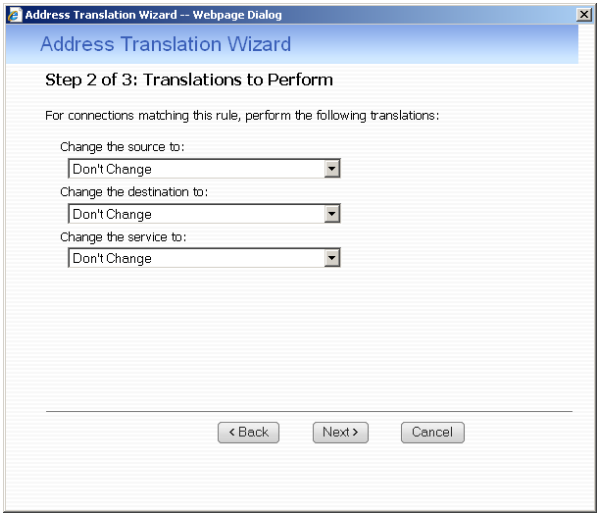
2. Do one of the following:
   - To add a new rule, click New.
   - To edit an existing rule, click next to the desired rule.

The Address Translation wizard opens, with the Step 1 of 3: Original Connection Details dialog box displayed.



3. Complete the fields using the relevant information in the following table.
4. Click Next.

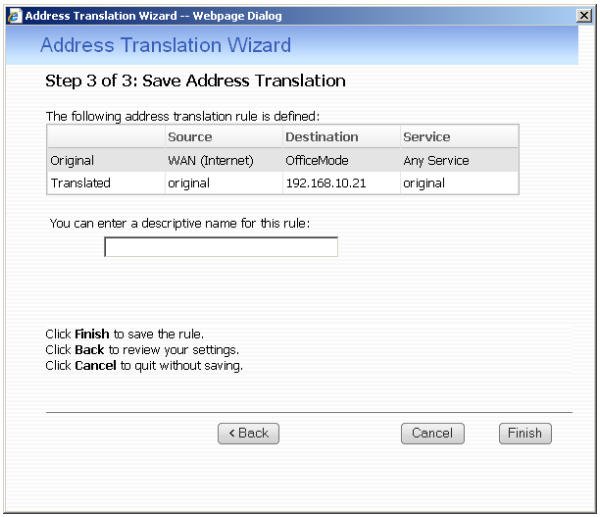
   The Step 2 of 3: Translations to Perform dialog box appears.


Address Translation Wizard -- Webpage Dialog
Address Translation Wizard
Step 2 of 3: Translations to Perform
For connections matching this rule, perform the following translations:
Change the source to:
Don't Change
Change the destination to:
Don't Change
Change the service to:
Don't Change
< Back
Next >
Cancel

5. Complete the fields using the relevant information in the following table.

6. Click Next.

   The Step 3 of 3: Save Address Translation dialog box appears.



7. If desired, type a description of the rule in the field provided.
8. Click Finish.

   The new rule appears in the Address Translation page.

Table 78: Address Translation Wizard Fields

Field	Description
The source is	Select the original source of the connections you want to translate. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.

Field	Description
And the destination is	Select the original destination of the connections you want to translate. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
And the service is	Select the original service used for the connections you want to translate. This list includes network service objects.
Change the source to	Select the new source to which the original source should be translated. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify that the original source should not be translated, select Don't Change.

Field	Description
Change the destination to	Select the new destination to which the original destination should be translated. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify that the original destination should not be translated, select Don't Change.
Change the service to	Select the new service to which the original service should be translated. This list includes network service objects. To specify that the original service should not be translated, select Don't Change.

Viewing and Deleting NAT Rules

500 1000N

This procedure explains how to view *all* NAT rules and how to delete *custom* NAT rules. You cannot delete implicitly defined NAT rules directly.

To view and delete NAT rules

1. Click Security in the main menu, and click the NAT tab.

   The Address Translation page appears with a list of all existing NAT rules.

   Implicitly defined NAT rules are marked Automatic Rule in the right-most column.

2. To delete a custom NAT rule, do the following.

   a. In the desired rule's row, click .
   A confirmation message appears.

b. Click OK.
The rule is deleted.

Using the EAP Authenticator

Wi-Fi Protected Access Enterprise (WPA-Enterprise) and 802.1x are Network Access Control (NAC) protocols that can be used to authenticate users connecting to the Check Point Safe@Office appliance. Both WPA-Enterprise and 802.1x can be used to control access to the wireless network; however, WPA-Enterprise has the added capability of encrypting transmitted data, and 802.1x can be used to secure connections to the Safe@Office appliance's LAN and DMZ ports as well.

Traditionally, WPA-Enterprise and 802.1x require installing an external Remote Authentication Dial-In User Service (RADIUS) server. When a user tries to authenticate using 802.1x or WPA-Enterprise, the Safe@Office appliance sends the entered user credentials to the RADIUS server. The server then checks whether the RADIUS database contains a matching set of credentials. If so, then the user is logged in.

While purchasing and configuring a RADIUS server may pose little challenge for a large enterprise, such a solution may be costly and complex, and may therefore be unsuitable for smaller networks. In such cases, it is recommended to configure the Safe@Office appliance's built-in Extended Authentication Protocol (EAP) authenticator, which allows using the local user database, enabling the use of WPA-Enterprise or 802.1x without an external RADIUS server.

Workflows

The Safe@Office built-in EAP authenticator can be used to authenticate wireless clients or wired clients connecting to appliance ports.

Using the EAP Authenticator for Authentication of Wireless Clients

500W 1000NW

To use the EAP authenticator for authentication of wireless clients

1. Configure the Safe@Office appliance as follows:

   a. Configure the desired wireless network for use with the EAP authenticator.

   For information on configuring the primary WLAN, see ***Manually Configuring a Wireless Network*** on page 321. For information on configuring a VAP, see ***Configuring Virtual Access Points*** on page 333.

Note: The Security field must set to 802.1x or WPA-Enterprise, and the Authentication Server field must be set to Internal User Database.

   b. Ensure that the Safe@Office appliance has a certificate installed in the Safe@Office Portal's VPN > Certificate page.

   The certificate can be any of the following:

   - A self-signed certificate generated by the Safe@Office appliance, version 8.0 or later.

     If a self-signed certificate is installed on the appliance, but was generated by an earlier firmware version, you must generate a new certificate. For instructions on generating a self-signed certificate, see ***Generating a Certificate*** on page 660.
   - A certificate received from the Service Center.

   c. Export the Safe@Office appliance's CA certificate.

   See ***Exporting the Safe@Office Appliance CA Certificate*** on page 669.

   d. For each client that should be allowed to connect to the Safe@Office appliance, add a user with Network Access permissions to the local user database.

See ***Adding and Editing Users*** on page 680.

e. Provide each of the users with the authentication credentials you configured for them.

2. Configure each wireless client as follows:

   a. Configure the client for server authentication.

   See ***Configuring Clients for Server Authentication on Wireless Connections*** on page 436.

   b. Install the Safe@Office appliance's CA certificate as a trusted root CA.

   See ***Installing the Safe@Office Appliance's CA Certificate on Clients*** on page 442.

3. Connect the wireless client to the wireless network.

   See ***Connecting Clients to the Safe@Office Appliance*** on page 447.

Using the EAP Authenticator for Authentication of Wired Clients

Power Pack

To use the EAP authenticator for authentication of wired clients

1. Configure the Safe@Office appliance as follows:

   a. Configure the desired port for port-based security using the Safe@Office EAP authenticator.

   See ***Configuring Port-Based Security*** on page 415.

Note: The Port Security field must set to 802.1x, and the Authentication Server field must be set to Internal User Database.

   b. Ensure that the Safe@Office appliance has a certificate installed in the Safe@Office Portal's VPN > Certificate page.

   The certificate can be any of the following:

   - A self-signed certificate generated by the Safe@Office appliance, version 8.0 or later.

     If a self-signed certificate is installed on the appliance, but was generated by an earlier firmware version, you must generate a new certificate. For

instructions on generating a self-signed certificate, see ***Generating a Certificate*** on page 660.

- A certificate received from the Service Center.

c. Export the Safe@Office appliance's CA certificate.

See ***Exporting the Safe@Office Appliance CA Certificate*** on page 669.

d. For each client that should be allowed to connect to the Safe@Office appliance, add a user with Network Access permissions to the local user database.

See ***Adding and Editing Users*** on page 680.

e. Provide each of the users with the authentication credentials you configured for them.

2. Configure each wired client as follows:

a. Configure the client for server authentication.

See ***Configuring Clients for Server Authentication on Wired Connections*** on page 440.

b. Install the Safe@Office appliance's CA certificate as a trusted root CA.

See ***Installing the Safe@Office Appliance's CA Certificate on Clients*** on page 442.

3. Connect the client directly to the port, and enter the Network Access user's authentication credentials when prompted.

Configuring Clients for Server Authentication on Wireless Connections

500W 1000NW

To configure a Microsoft Windows client for server authentication

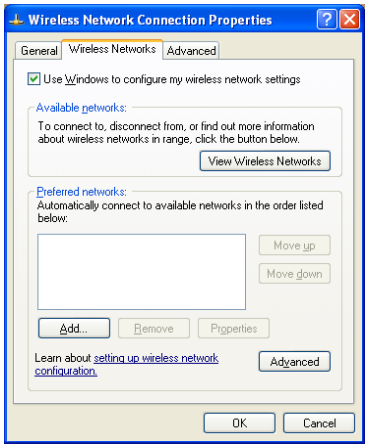
1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Double-click on the wireless network connection.
4. Do one of the following:

- If the Choose a Wireless Network screen appears, click Change Advanced Settings.
- If you are already connected to a wireless network, click Properties.

The Wireless Network Connection Properties dialog box appears displaying the General tab.

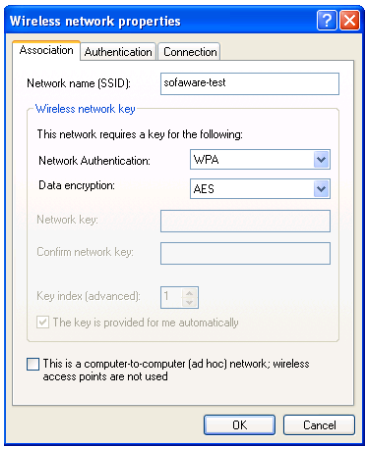
5. Click the Wireless Networks tab.

   The Wireless Networks tab appears.



6. Click Add and add your network.

   The Wireless network properties dialog box appears displaying the Association tab.

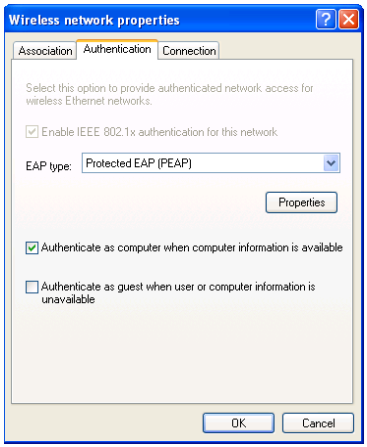


7. In the Network name (SSID) field, type the Safe@Office appliance wireless network name.
8. In the Network Authentication drop-down list, select WPA.

Note: You must select WPA, regardless of whether the Safe@Office appliance is configured to use the WPA-Enterprise or 802.1x security protocol.

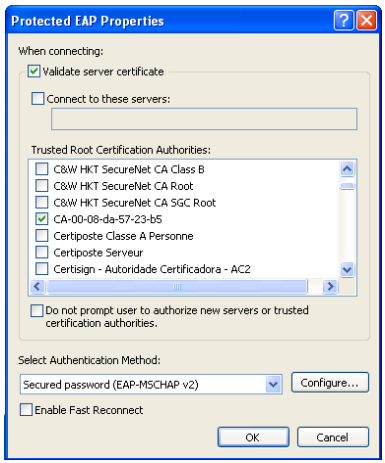
9. In the Data encryption drop-down list, select AES.
10. Click the Authentication tab.

    The Authentication tab appears.



11. In the EAP type drop-down list, select Protected EAP (PEAP).
12. Select the Authenticate as computer when computer information is available check box.
13. Click Properties.

The Protected EAP Properties dialog box appears.



14. Make sure that the Validate server certificate check box is selected.
15. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
16. If the user credentials for connecting to the Safe@Office appliance differ from the user credentials for connecting to Windows, do the following:
    a. Click Configure.
       The EAP MSCHAPv2 Properties dialog box appears.

    b. Clear the check box.
    c. Click OK.
17. Click OK in all open windows.

Configuring Clients for Server Authentication on Wired Connections

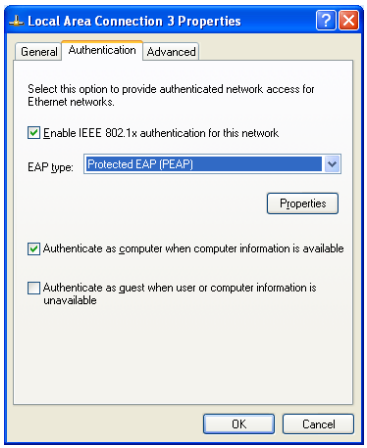
Power Pack

To configure a Microsoft Windows client for server authentication

1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Right-click on Local Area Connection, and click Properties in the popup menu that appears.

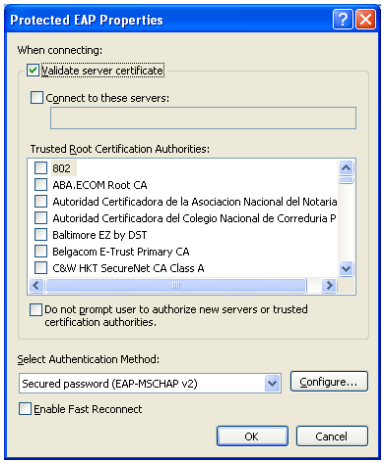
   The Local Area Connection Properties dialog box appears displaying the General tab.
4. Click the Authentication tab.

   The Authentication tab appears.


Local Area Connection 3 Properties
General
Authentication
Advanced
Select this option to provide authenticated network access for Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Protected EAP (PEAP)
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

5. Select the Enable IEEE 802.1x authentication for this network check box.
6. In the EAP type drop-down list, select Protected EAP (PEAP).
7. Select the Authenticate as computer when computer information is available check box.
8. Click Properties.

The Protected EAP Properties dialog box appears.



9. Make sure that the Validate server certificate check box is selected.
10. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
11. If the user credentials for connecting to the Safe@Office appliance differ from the user credentials for connecting to Windows, do the following:
    a. Click Configure.
       The EAP MSCHAPv2 Properties dialog box appears.

    b. Clear the check box.
    c. Click OK.
12. Click OK in all open windows.

Installing the Safe@Office Appliance's CA Certificate on Clients

500 1000N

To install the Safe@Office appliance's CA certificate on a Microsoft Windows client

1. On the client, right-click on the Safe@Office appliance's CA certificate you exported, and click Install PFX in the pop-up menu that appears.

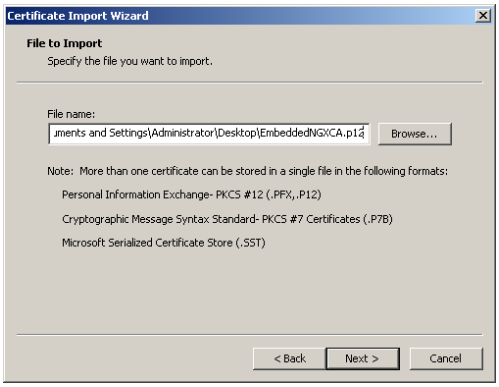
   For information on exporting the CA certificate, see ***Exporting the Safe@Office Appliance CA Certificate*** on page 669.

   The Certificate Import Wizard opens displaying the Welcome to Certificate Import Wizard screen.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

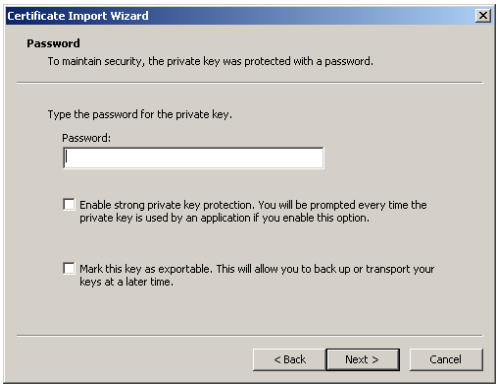
2. Click Next.

The File to Import dialog box appears.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
uments and Settings\Administrator\Desktop\EmbeddedNGXCA.p12
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

3. Browse to the Safe@Office appliance's CA certificate (*.p12 file).
4. Click Next.

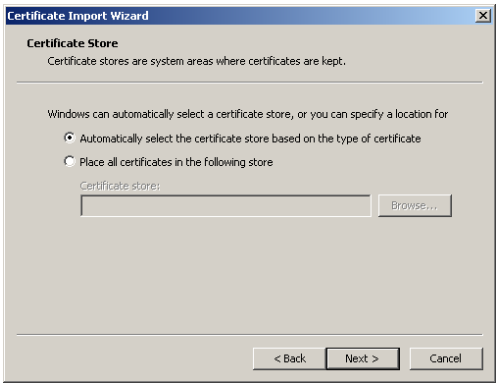
   The Password dialog box appears.


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
< Back
Next >
Cancel

   Do not type a password.

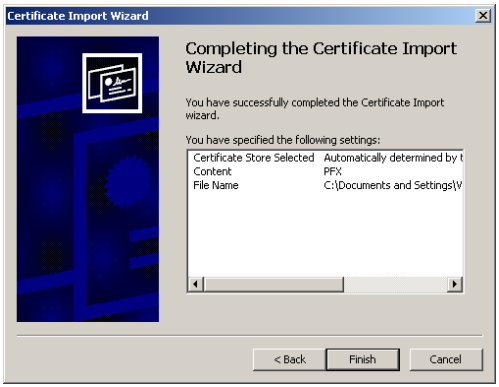
5. Click Next.

The **Certificate Store** dialog box appears.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

6. Click **Automatically select the certificate store based on the type of certificate.**
7. Click **Next.**

   The **Completing the Certificate Import Wizard** screen appears.



8. Click **Finish.**

If the Safe@Office appliance certificate was self-signed, a warning message appears.

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
CA-00:08:da:77:70:70
Windows cannot validate that the certificate is actually from "CA-00:08:da:77:70:70". You should confirm its origin by contacting "CA-00:08:da:77:70:70". The following number will assist you in this process:
Thumbprint (sha1): 4240E3F0 A7EE46B7 D8CE5150 6763C48D 43D33F40
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Do the following:

a. Click Yes.

   A success message appears.

b. Click OK.

9. To check that the certificate was successfully installed as a trusted root CA, do the following:

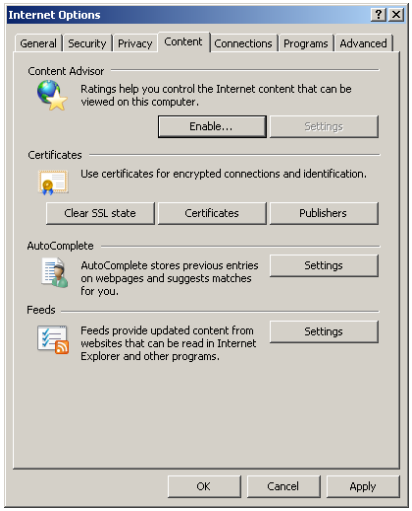
   a. On the client, open Internet Explorer.

   b. In the Tools menu, click Internet Options.

      The Internet Options dialog box appears displaying the General tab.

   c. Click the Content tab.

      The Content tab appears.

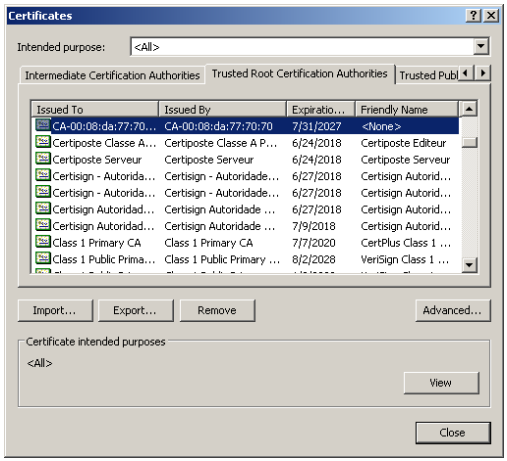


d. Click Certificates.

The Certificates dialog box appears.

e. Click the Trusted Root Certification Authorities tab.

The Trusted Root Certification Authorities tab appears.

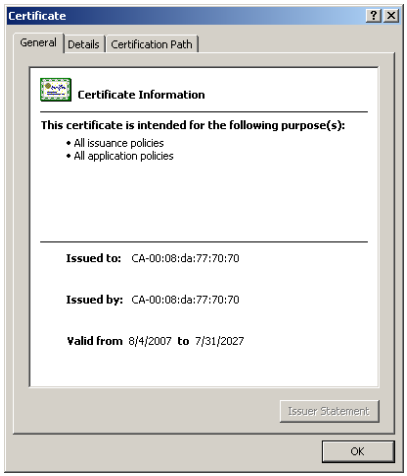


f. In the list, locate the Safe@Office appliance's CA certificate.

The certificate's name is in the format `CA-<Identifier>`, where `<Identifier>` is the Safe@Office appliance's MAC address or gateway name.

g. To view further information about the certificate, double-click on it.

The Certificate dialog box appears with additional information.



Connecting Wireless Clients to the Safe@Office Appliance

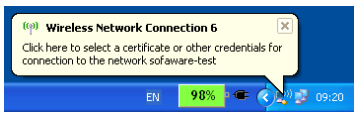
500W 1000NW

To connect a Microsoft Windows wireless client to the Safe@Office appliance with WPA Enterprise authentication

1. In the START menu, click Control Panel.
2. Click Network Connections.

   A list of wireless networks appears.
3. Select the Safe@Office appliance wireless network.
4. Click Connect.

   A popup message appears asking you to supply credentials.


Wireless Network Connection 6
Click here to select a certificate or other credentials for connection to the network sofaware-test
EN
98%
09:20

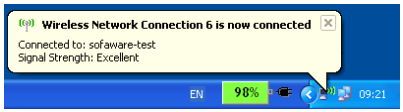
5. Click on the popup message.

The Enter Credentials dialog box appears.

6. Type the Network Access user's user name and password in the fields provided.
7. Click OK.

   The wireless client attempts to connect to the network.

   Upon successful connection, the client indicates that it is connected to the network.



Chapter 14

Using SmartDefense

This chapter explains how to use Check Point SmartDefense Services.

This chapter includes the following topics:

Overview 449
Configuring SmartDefense 450
SmartDefense Categories 458
Resetting SmartDefense to its Defaults 503

Overview

The Safe@Office appliance includes Check Point SmartDefense Services, based on Check Point Application Intelligence. SmartDefense provides a combination of attack safeguards and attack-blocking tools that protect your network in the following ways:

- Validating compliance to standards
- Validating expected usage of protocols (Protocol Anomaly Detection)
- Limiting application ability to carry malicious data
- Controlling application-layer operations

In addition, SmartDefense aids proper usage of Internet resources, such as FTP, instant messaging, Peer-to-Peer (P2P) file sharing, file-sharing operations, and File Transfer Protocol (FTP) uploading, among others.

Configuring SmartDefense

500 1000N

You can configure SmartDefense using the following tools:

- SmartDefense Wizard. Resets all SmartDefense settings to their defaults, and then creates a SmartDefense security policy according to your network and security preferences. See ***Using the SmartDefense Wizard*** on page 450.
- SmartDefense Tree. Enables you to fine tune individual settings in the SmartDefense policy. You can use the SmartDefense tree instead of, or in addition to, the wizard. See ***Using the SmartDefense Tree*** on page 456.

Using the SmartDefense Wizard

500 1000N

The SmartDefense Wizard allows you to configure your SmartDefense security policy quickly and easily through its user-friendly interface.

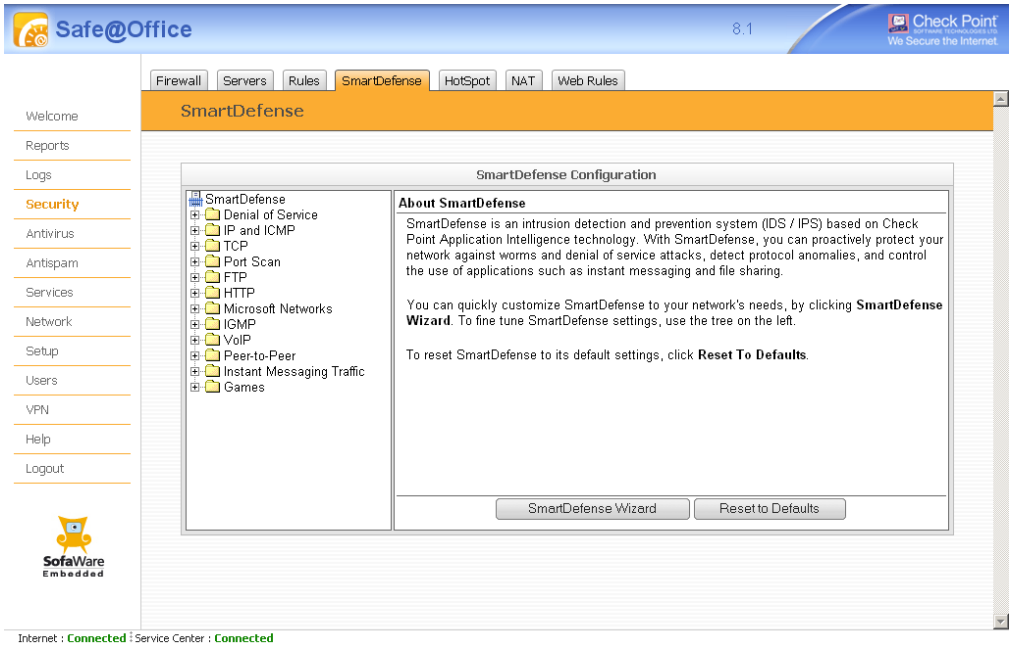
Note: The SmartDefense wizard clears any existing SmartDefense settings.

After using the wizard, you can fine tune the policy settings using the SmartDefense tree. See ***Using the SmartDefense Tree*** on page 456.

To configure the SmartDefense policy using the wizard

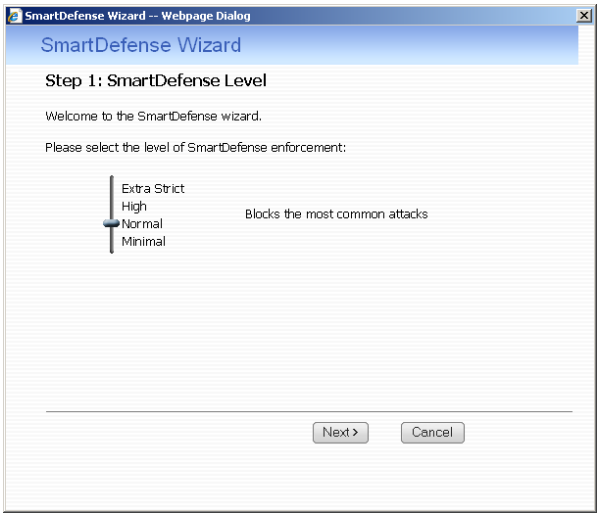
1. Click Security in the main menu, and click the SmartDefense tab.

The SmartDefense page appears.



2. Click SmartDefense Wizard.

The SmartDefense Wizard opens, with the Step 1: SmartDefense Level dialog box displayed.

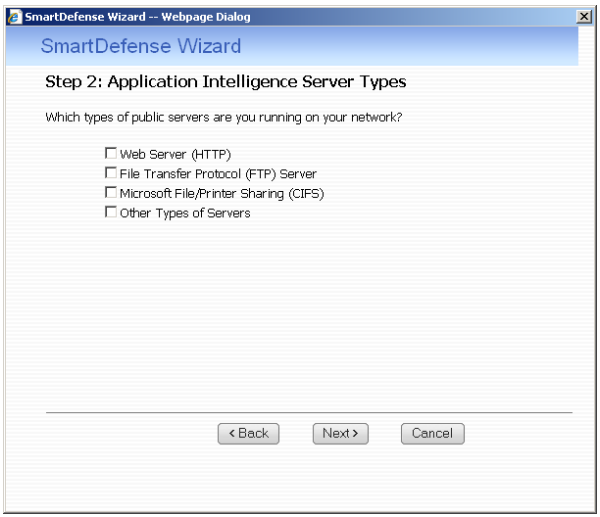


3. Drag the lever to the desired level of SmartDefense enforcement.

   For information on the levels, see the following table.

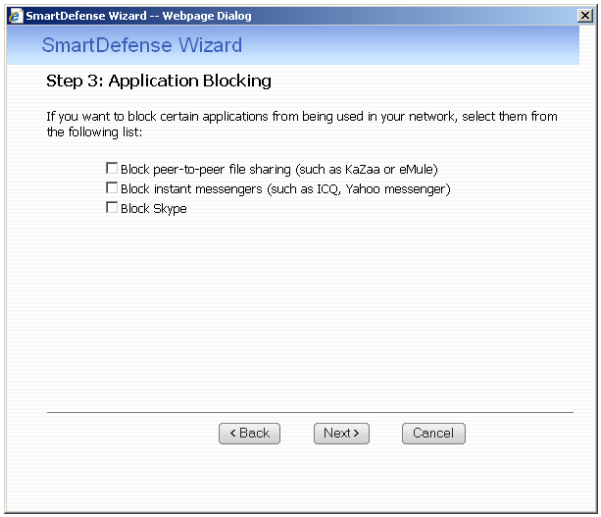
4. Click Next.

   The Step 2: Application Intelligence Server Types dialog box appears.


SmartDefense Wizard -- Webpage Dialog
SmartDefense Wizard
Step 2: Application Intelligence Server Types
Which types of public servers are you running on your network?
Web Server (HTTP)
File Transfer Protocol (FTP) Server
Microsoft File/Printer Sharing (CIFS)
Other Types of Servers
< Back
Next >
Cancel

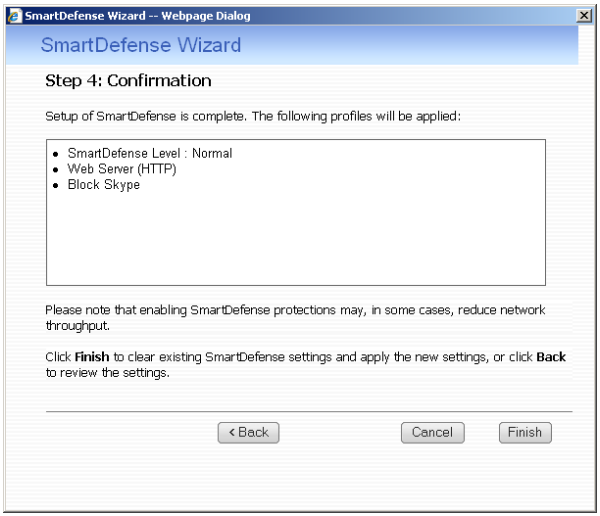
5. Select the check boxes next to the types of public servers that are running on your network.
6. Click Next.

   The Step 3: Application Blocking dialog box appears.


SmartDefense Wizard -- Webpage Dialog
SmartDefense Wizard
Step 3: Application Blocking
If you want to block certain applications from being used in your network, select them from the following list:
Block peer-to-peer file sharing (such as KaZaa or eMule)
Block instant messengers (such as ICQ, Yahoo messenger)
Block Skype
< Back
Next >
Cancel

7. Select the check boxes next to the types of applications you want to block from running on your network.
8. Click Next.

The Step 4: Confirmation dialog box appears.


SmartDefense Wizard -- Webpage Dialog
SmartDefense Wizard
Step 4: Confirmation
Setup of SmartDefense is complete. The following profiles will be applied:
SmartDefense Level : Normal
Web Server (HTTP)
Block Skype
Please note that enabling SmartDefense protections may, in some cases, reduce network throughput.
Click Finish to clear existing SmartDefense settings and apply the new settings, or click Back to review the settings.
< Back
Cancel
Finish

9. Click Finish.

   Existing SmartDefense settings are cleared, and the security policy is applied.

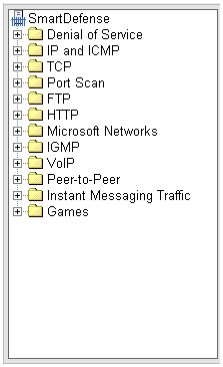
Table 79: SmartDefense Security Levels

This level...	Does this...
Minimal	Disables all SmartDefense protections, except those that cannot be disabled.
Normal	Enables the following: • Teardrop • Ping of Death • LAND • Packet Sanity • Max Ping Size (set to 1500) • Welchia • Cisco IOS • Null Payload • IGMP • Small PMTU (Log Only) This level blocks the most common attacks.
High	Enables the same protections as Normal level, as well as the following: • Host Port Scan • Sweep Scan • HTTP Header Rejection • Strict TCP (Log Only)
Extra Strict	Enables the same protections as High level, as well as the following: • Strict TCP (Log + Block) • Small PMTU (Log + Block) • Max Ping Size (set to 512) • Network Quota

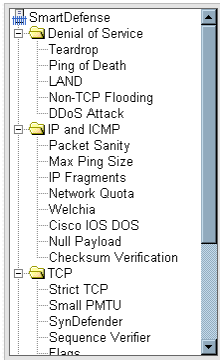
Using the SmartDefense Tree

500 1000N

For convenience, SmartDefense is organized as a tree, in which each branch represents a category of settings.



When a category is expanded, the settings it contains appear as nodes. For information on each category and the nodes it contains, see ***SmartDefense Categories*** on page 458.



Each node represents an attack type, a sanity check, or a protocol or service that is vulnerable to attacks. To control how SmartDefense handles a specific attack, you must configure the relevant node's settings.

To configure a SmartDefense node

1. Click Security in the main menu, and click the SmartDefense tab.

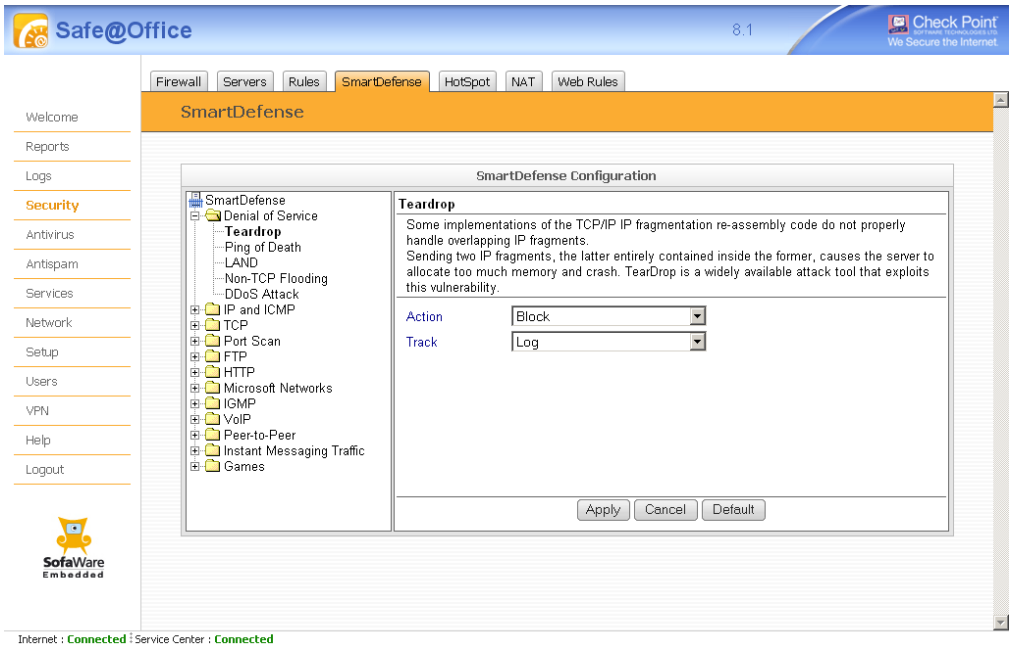
   The SmartDefense page appears.

   The left pane displays a tree containing SmartDefense categories.

   - To expand a category, click the ⊞ icon next to it.
   - To collapse a category, click the ⊟ icon next to it.

2. Expand the relevant category, and click on the desired node.

   The right pane displays a description of the node, followed by fields.



3. To modify the node's current settings, do the following:

   a) Complete the fields using the relevant information in ***SmartDefense Categories*** on page 458.

   b) Click Apply.

4. To reset the node to its default values:

a) Click Default.
   A confirmation message appears.
b) Click OK.
   The fields are reset to their default values, and your changes are saved.

SmartDefense Categories

SmartDefense includes the following categories:

- ***Denial of Service*** on page 458
- ***FTP*** on page 485
- ***HTTP*** on page 490
- ***IGMP*** on page 494
- ***Instant Messaging Traffic*** on page 500
- ***IP and ICMP*** on page 464
- ***Microsoft Networks*** on page 492
- ***Peer-to-Peer*** on page 498
- ***Port Scan*** on page 483
- ***TCP*** on page 476
- ***VoIP*** on page 495
- ***Games*** on page 502

Denial of Service

Denial of Service (DoS) attacks are aimed at overwhelming the target with spurious data, to the point where it is no longer able to respond to legitimate service requests.

This category includes the following attacks:

- ***DDoS Attack*** on page 463
- ***LAND*** on page 461
- ***Non-TCP Flooding*** on page 462

- ***Ping of Death*** on page 460
- ***Teardrop*** on page 459

Teardrop

In a Teardrop attack, the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.

You can configure how Teardrop attacks should be handled.

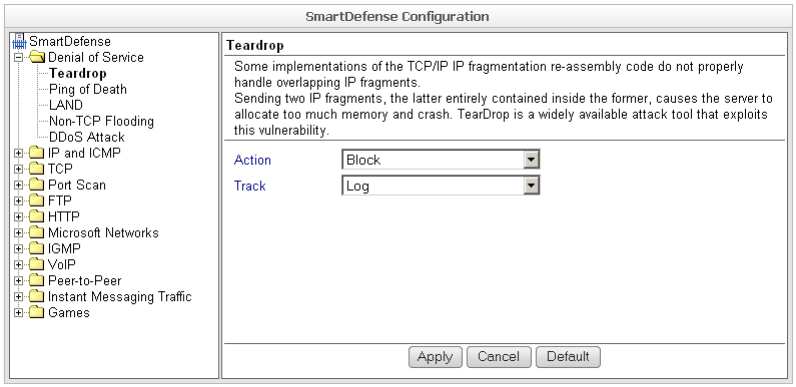


Table 80: Teardrop Fields

In this field...	Do this...
Action	Specify what action to take when a Teardrop attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Teardrop attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Ping of Death

In a Ping of Death attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash.

You can configure how Ping of Death attacks should be handled.

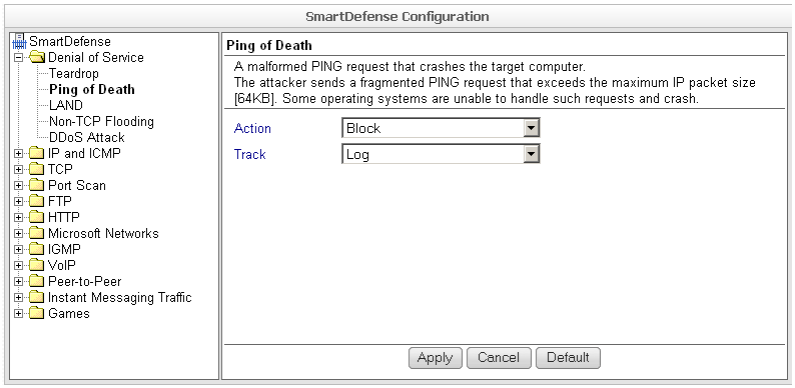


Table 81: Ping of Death Fields

In this field…	Do this…
Action	Specify what action to take when a Ping of Death attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Ping of Death attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

LAND

In a LAND attack, the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.

You can configure how LAND attacks should be handled.

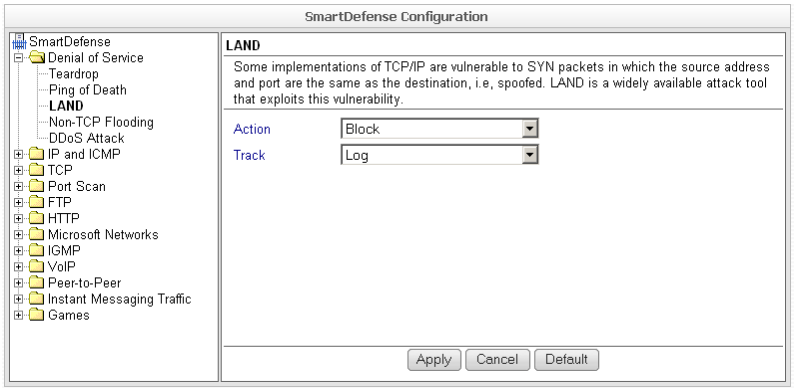


Table 82: LAND Fields

In this field...	Do this...
Action	Specify what action to take when a LAND attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log LAND attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Non-TCP Flooding

Advanced firewalls maintain state information about connections in a State table. In Non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).

You can protect against Non-TCP Flooding attacks by limiting the percentage of state table capacity used for non-TCP connections.

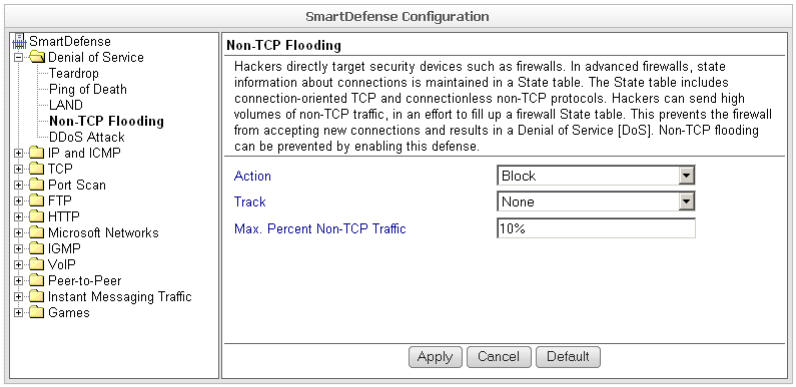

SmartDefense Configuration
SmartDefense
Denial of Service
Teardrop
Ping of Death
LAND
Non-TCP Flooding
DDoS Attack
IP and ICMP
TCP
Port Scan
FTP
HTTP
Microsoft Networks
IGMP
VoIP
Peer-to-Peer
Instant Messaging Traffic
Games
Non-TCP Flooding
Hackers directly target security devices such as firewalls. In advanced firewalls, state information about connections is maintained in a State table. The State table includes connection-oriented TCP and connectionless non-TCP protocols. Hackers can send high volumes of non-TCP traffic, in an effort to fill up a firewall State table. This prevents the firewall from accepting new connections and results in a Denial of Service [DoS]. Non-TCP flooding can be prevented by enabling this defense.
Action
Block
Track
None
Max. Percent Non-TCP Traffic
10%
Apply
Cancel
Default

Table 83: Non-TCP Flooding Fields

In this field…	Do this…
Action	Specify what action to take when the percentage of state table capacity used for non-TCP connections reaches the Max. percent non TCP traffic threshold. Select one of the following: • Block. Block any additional non-TCP connections. • None. No action. This is the default.
Track	Specify whether to log non-TCP connections that exceed the Max. Percent Non-TCP Traffic threshold, by selecting one of the following: • Log. Log the connections. • None. Do not log the connections. This is the default.

In this field...	Do this...
Max. Percent Non-TCP Traffic	Type the maximum percentage of state table capacity allowed for non-TCP connections. The default value is 10%.

DDoS Attack

In a distributed denial-of-service attack (DDoS attack), the attacker directs multiple hosts in a coordinated attack on a victim computer or network. The attacking hosts send large amounts of spurious data to the victim, so that the victim is no longer able to respond to legitimate service requests.

You can configure how DDoS attacks should be handled.

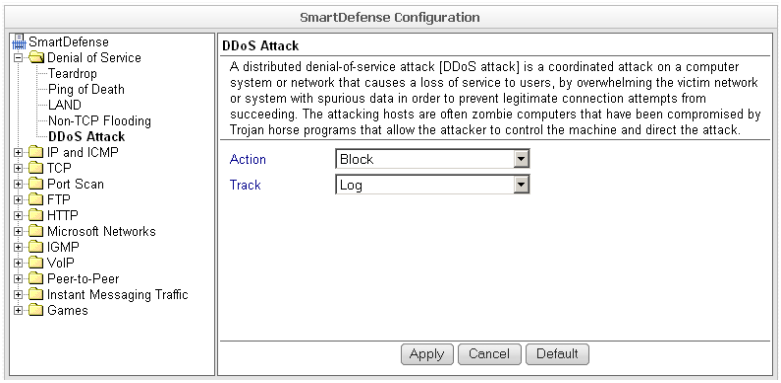

SmartDefense Configuration
SmartDefense
Denial of Service
Teardrop
Ping of Death
LAND
Non-TCP Flooding
DDoS Attack
IP and ICMP
TCP
Port Scan
FTP
HTTP
Microsoft Networks
IGMP
VoIP
Peer-to-Peer
Instant Messaging Traffic
Games
DDoS Attack
A distributed denial-of-service attack [DDoS attack] is a coordinated attack on a computer system or network that causes a loss of service to users, by overwhelming the victim network or system with spurious data in order to prevent legitimate connection attempts from succeeding. The attacking hosts are often zombie computers that have been compromised by Trojan horse programs that allow the attacker to control the machine and direct the attack.
Action
Block
Track
Log
Apply
Cancel
Default

Table 84: Distributed Denial of Service Fields

In this field...	Do this...
Action	Specify what action to take when a DDoS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log DDoS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

IP and ICMP

This category allows you to enable various IP and ICMP protocol tests, and to configure various protections against IP and ICMP-related attacks. It includes the following:

- ***Checksum Verification*** on page 475
- ***Cisco IOS DOS*** on page 472
- ***IP Fragments*** on page 468
- ***Max Ping Size*** on page 467
- ***Network Quota*** on page 470
- ***Null Payload*** on page 474
- ***Packet Sanity*** on page 465
- ***Welchia*** on page 471

Packet Sanity

Packet Sanity performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

You can configure whether logs should be issued for offending packets.

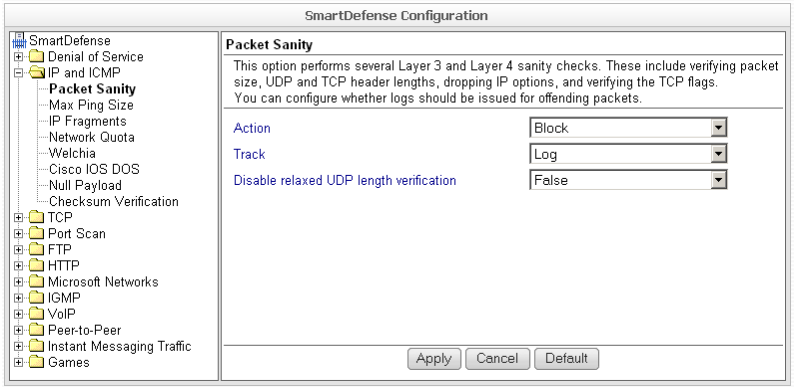


Table 85: Packet Sanity Fields

In this field...	Do this...
Action	Specify what action to take when a packet fails a sanity test, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action.
Track	Specify whether to issue logs for packets that fail the packet sanity tests, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.

In this field...	Do this...
Disable relaxed UDP length verification	The UDP length verification sanity check measures the UDP header length and compares it to the UDP header length specified in the UDP header. If the two values differ, the packet may be corrupted. However, since different applications may measure UDP header length differently, the Safe@Office appliance relaxes the UDP length verification sanity check by default, performing the check but not dropping offending packets. This is called relaxed UDP length verification. Specify whether the Safe@Office appliance should relax the UDP length verification sanity check or not, by selecting one of the following: • True. Disable relaxed UDP length verification. The Safe@Office appliance will drop packets that fail the UDP length verification check. • False. Do not disable relaxed UDP length verification. The Safe@Office appliance will not drop packets that fail the UDP length verification check. This is the default.

Max Ping Size

PING (ICMP echo request) is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.

An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.

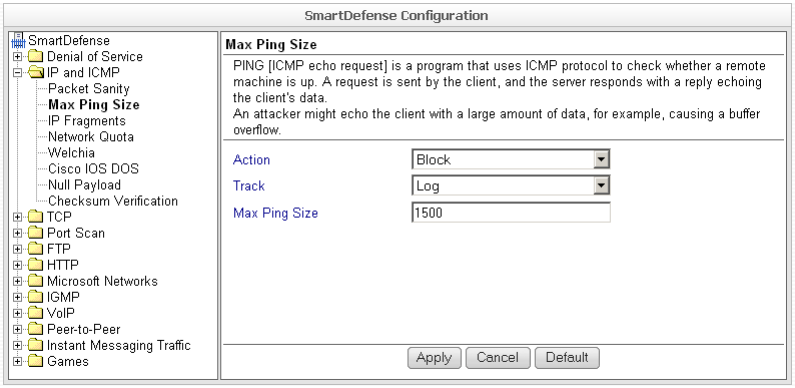


Table 86: Max Ping Size Fields

In this field...	Do this...
Action	Specify what action to take when an ICMP echo response exceeds the Max Ping Size threshold, by selecting one of the following: • Block. Block the request. This is the default. • None. No action.
Track	Specify whether to log ICMP echo responses that exceed the Max Ping Size threshold, by selecting one of the following: • Log. Log the responses. This is the default. • None. Do not log the responses.
Max Ping Size	Specify the maximum data size for ICMP echo response. The default value is 548.

IP Fragments

When an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behavior and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore, the Safe@Office appliance always reassembles all the fragments of a given IP packet, before inspecting it to make sure there are no attacks or exploits in the packet.

You can configure how fragmented packets should be handled.

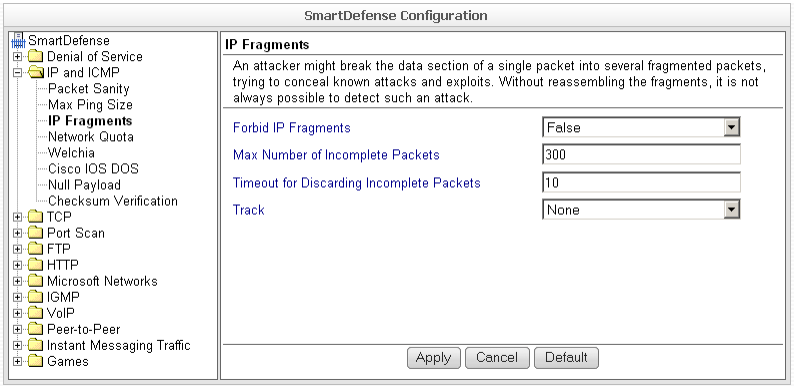


Table 87: IP Fragments Fields

In this field...	Do this...
Forbid IP Fragments	Specify whether all fragmented packets should be dropped, by selecting one of the following: • True. Drop all fragmented packets. • False. No action. This is the default. Under normal circumstances, it is recommended to leave this field set to False. Setting this field to True may disrupt Internet connectivity, because it does not allow any fragmented packets.
Max Number of Incomplete Packets	Type the maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. The default value is 300.
Timeout for Discarding Incomplete Packets	When the Safe@Office appliance receives packet fragments, it waits for additional fragments to arrive, so that it can reassemble the packet. Type the number of seconds to wait before discarding incomplete packets. The default value is 10.
Track	Specify whether to log fragmented packets, by selecting one of the following: • Log. Log all fragmented packets. • None. Do not log the fragmented packets. This is the default.

Network Quota

An attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial Of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

You can configure how connections that exceed that limit should be handled.

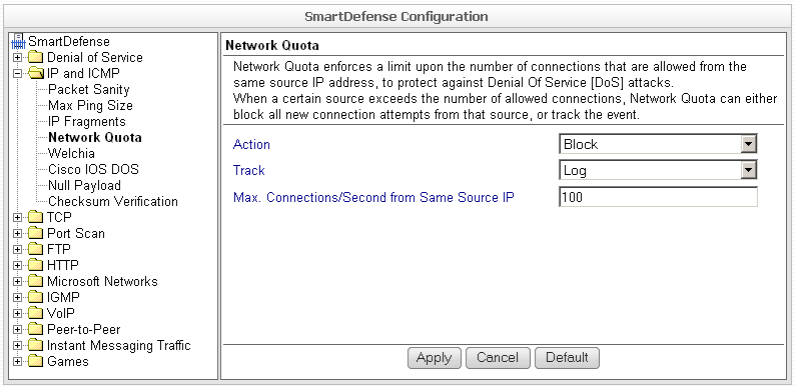


Table 88: Network Quota Fields

In this field...	Do this...
Action	Specify what action to take when the number of network connections from the same source reaches the Max. Connections/Second per Source IP threshold. Select one of the following: • Block. Block all new connections from the source. Existing connections will not be blocked. This is the default. • None. No action.
Track	Specify whether to log connections from a specific source that exceed the Max. Connections/Second per Source IP threshold, by selecting one of the following: • Log. Log the connections. This is the default. • None. Do not log the connections.

In this field...	Do this...
Max. Connections/Second from Same Source IP	Type the maximum number of network connections allowed per second from the same source IP address. The default value is 100. Set a lower threshold for stronger protection against DoS attacks. Note: Setting this value too low can lead to false alarms.

Welchia

The Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

You can configure how the Welchia worm should be handled.

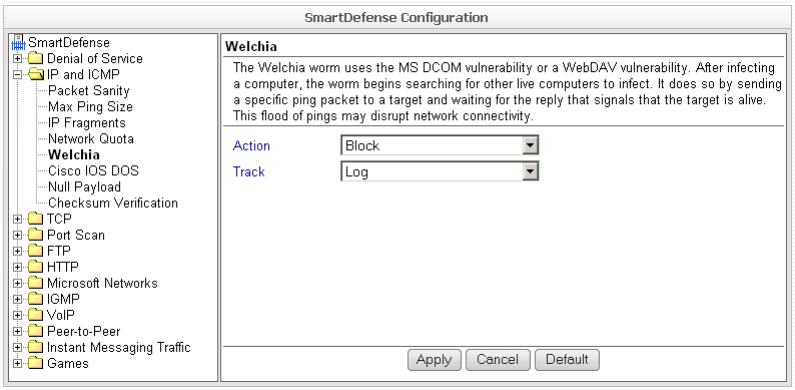


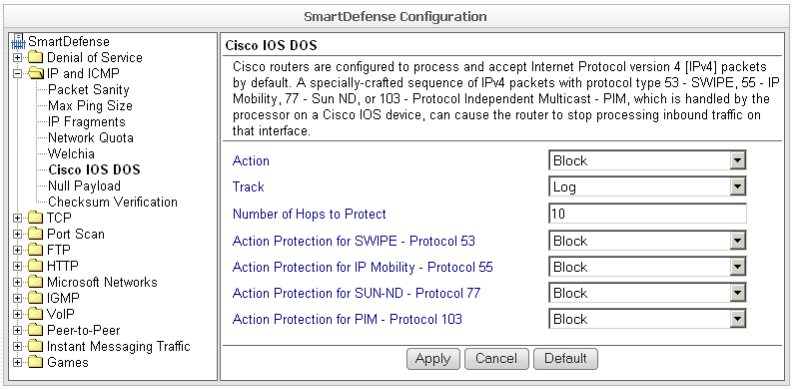
Table 89: Welchia Fields

In this field…	Do this…
Action	Specify what action to take when the Welchia worm is detected, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Welchia worm attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Cisco IOS DOS

Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. When a Cisco IOS device is sent a specially crafted sequence of IPv4 packets (with protocol type 53 - SWIPE, 55 - IP Mobility, 77 - Sun ND, or 103 - Protocol Independent Multicast - PIM), the router will stop processing inbound traffic on that interface.

You can configure how Cisco IOS DOS attacks should be handled.



Note: You cannot enable CISCO IOS DOS PIM protection in SmartDefense, when the PIM-SM multicast routing protocol is enabled. For information on disabling the PIM-SM protocol, refer to the *Embedded NGX CLI Reference Guide*.

Table 90: Cisco IOS DOS

In this field...	Do this...
Action	Specify what action to take when a Cisco IOS DOS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Cisco IOS DOS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.
Number of Hops to Protect	Type the number of hops from the enforcement module that Cisco routers should be protected. The default value is 10.
Action Protection for SWIPE - Protocol 53 / IP Mobility - Protocol 55 / SUN-ND - Protocol 77 / PIM - Protocol 103	Specify what action to take when an IPv4 packet of the specific protocol type is received, by selecting one of the following: • Block. Drop the packet. This is the default. • None. No action.

Null Payload

Some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.

You can configure how null payload ping packets should be handled.

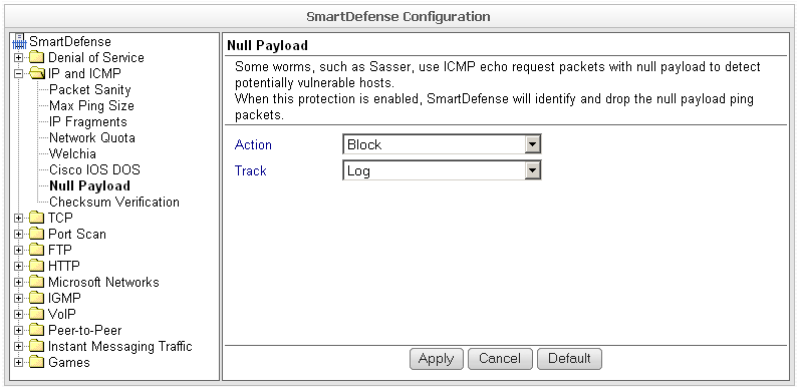


Table 91: Null Payload Fields

In this field…	Do this…
Action	Specify what action to take when null payload ping packets are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Checksum Verification

SmartDefense identifies any IP, TCP, or UDP packets with incorrect checksums. You can configure how these packets should be handled.

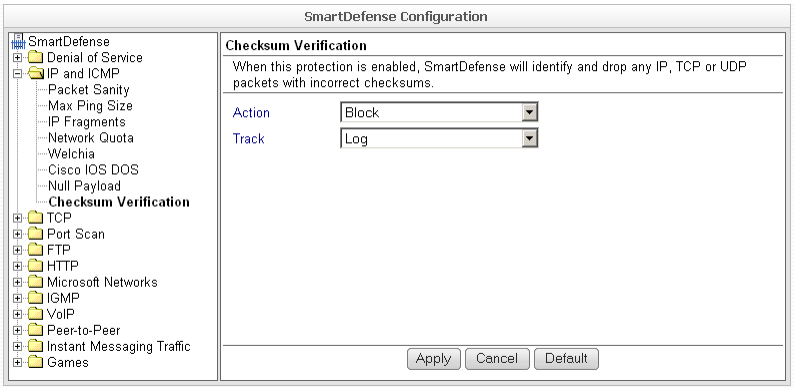


Table 92: Checksum Verification Fields

In this field...	Do this...
Action	Specify what action to take when packets with incorrect checksums are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log packets with incorrect checksums, by selecting one of the following: • Log. Log the packets. • None. Do not log the packets. This is the default.

TCP

This category allows you to configure various protections related to the TCP protocol. It includes the following:

- ***Flags*** on page 482
- ***Sequence Verifier*** on page 481
- ***Small PMTU*** on page 477
- ***Strict TCP*** on page 476
- ***SynDefender*** on page 479

Strict TCP

Out-of-state TCP packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet.

Note: In normal conditions, out-of-state TCP packets can occur after the Safe@Office restarts, since connections which were established prior to the reboot are unknown. This is normal and does not indicate an attack.

Note: Certain SmartDefense protections implicitly apply the Strict TCP protection to relevant connections. In such cases, "TCP Out-of-State" log messages may appear in the Security Log, even though the Strict TCP protection is disabled.

You can configure how out-of-state TCP packets should be handled.

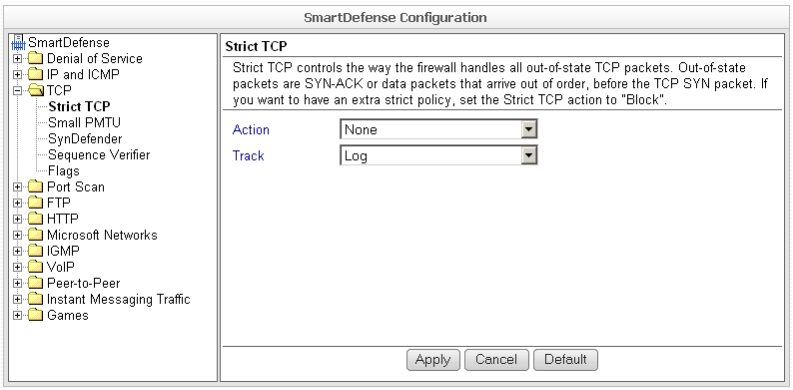


Table 93: Strict TCP

In this field...	Do this...
Action	Specify what action to take when an out-of-state TCP packet arrives, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Small PMTU

Small PMTU (Packet MTU) is a bandwidth attack in which the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a "bottleneck" on the server.

You can protect against this attack by specifying a minimum packet size for data sent over the Internet.

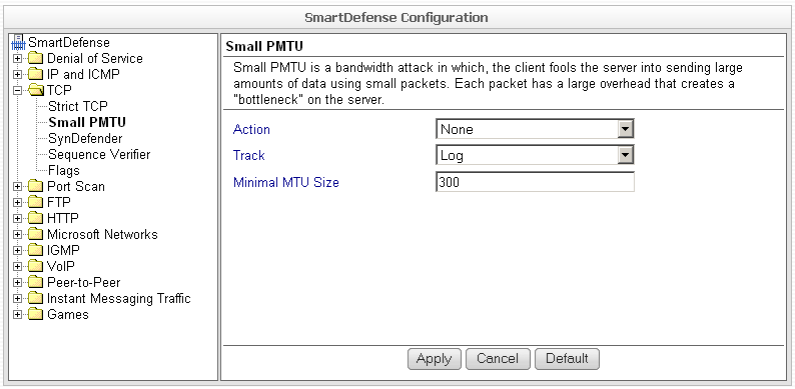


Table 94: Small PMTU Fields

In this field…	Do this…
Action	Specify what action to take when a packet is smaller than the Minimal MTU Size threshold, by selecting one of the following: • Block. Block the packet. • None. No action. This is the default.
Track	Specify whether to issue logs for packets are smaller than the Minimal MTU Size threshold, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.
Minimal MTU Size	Type the minimum value allowed for the MTU field in IP packets sent by a client. An overly small value will not prevent an attack, while an overly large value might degrade performance and cause legitimate requests to be dropped. The default value is 300.

SynDefender

In a SYN attack, the attacker sends many SYN packets without finishing the three-way handshake. This causes the attacked host to be unable to accept new connections.

You can protect against this attack by specifying a maximum amount of time for completing handshakes.

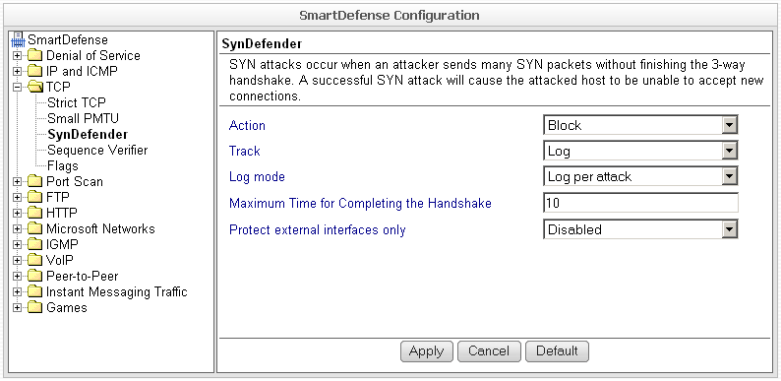


Table 95: SynDefender Fields

In this field...	Do this...
Action	Specify what action to take when a SYN attack occurs, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action. A SYN attack is when more than 5 incomplete TCP handshakes are detected within 10 seconds. A handshake is considered incomplete when it exceeds the Maximum time for completing the handshake threshold.
Track	Specify whether to issue logs for the events specified by the Log Mode parameter, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.

In this field...	Do this...
Log mode	Specify upon which events logs should be issued, by selecting one of the following: • None. Do not issue logs. • Log per attack. Issue logs for each SYN attack. This is the default. • Log individual unfinished handshakes. Issue logs for each incomplete handshake. This field is only relevant if the Track field is set to Log.
Maximum Time for Completing the Handshake	Type the maximum amount of time in seconds after which a TCP handshake is considered incomplete. The default value is 10 seconds.
Protect external interfaces only	Specify whether SynDefender should be enabled for external (WAN) interfaces only, by selecting one of the following: • Disabled. Enable SynDefender for all the firewall interfaces. This is the default. • Enabled. Enable SynDefender for external interfaces only.

Sequence Verifier

The Safe@Office appliance examines each TCP packet's sequence number and checks whether it matches a TCP connection state. You can configure how the appliance handles packets that match a TCP connection in terms of the TCP session but have incorrect sequence numbers.

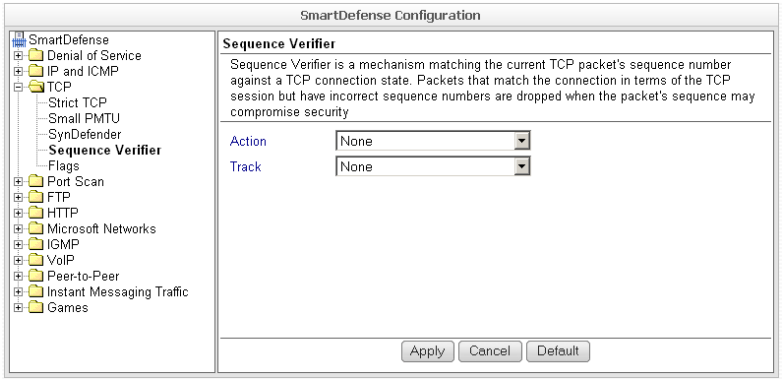


Table 96: Strict TCP

In this field...	Do this...
Action	Specify what action to take when TCP packets with incorrect sequence numbers arrive, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log TCP packets with incorrect sequence numbers, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Flags

The URG flag is used to indicate that there is urgent data in the TCP stream, and that the data should be delivered with high priority. Since handling of the URG flag is inconsistent between different operating systems, an attacker can use the URG flag to conceal certain attacks.

You can configure how the URG flag should be handled.

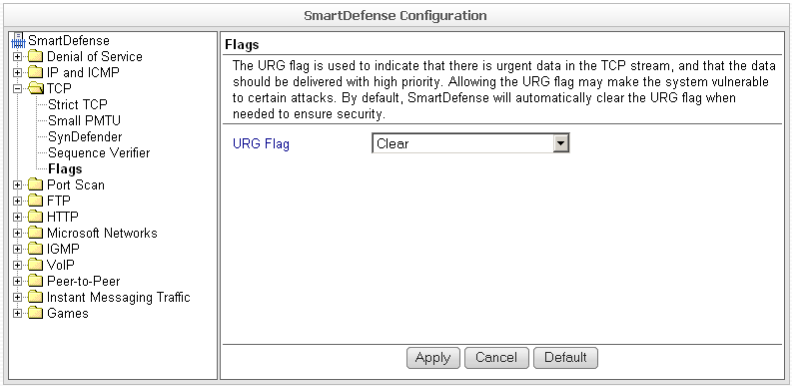


Table 97: Flags Fields

In this field…	Do this…
URG Flag	Specify whether to clear or allow the URG flag, by selecting one of the following: • Clear. Clear the URG flag on all incoming packets. This is the default. • Allow. Allow the URG flag.

Port Scan

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open.

This category includes the following types of port scans:

- Host Port Scan. The attacker scans a specific host's ports to determine which of the ports are open.
- Sweep Scan. The attacker scans various hosts to determine where a specific port is open.

You can configure how the Safe@Office appliance should react when a port scan is detected.

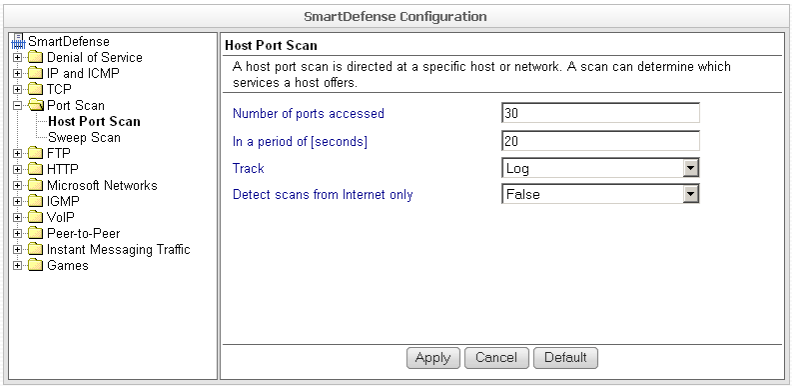


Table 98: Port Scan Fields

In this field...	Do this...
Number of ports accessed	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the minimum number of ports that must be accessed within the In a period of [seconds] period, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 30, and 40 ports are accessed within a specified period of time, SmartDefense will detect the activity as a port scan. For Host Port Scan, the default value is 30. For Sweep Scan, the default value is 50.
In a period of [seconds]	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the maximum number of seconds that can elapse, during which the Number of ports accessed threshold is exceeded, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 20, and the Number of ports accessed threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan. The default value is 20 seconds.

In this field...	Do this...
Track	Specify whether to issue logs for scans, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs. This is the default.
Detect scans from Internet only	Specify whether to detect only scans originating from the Internet, by selecting one of the following: • False. Do not detect only scans from the Internet. This is the default. • True. Detect only scans from the Internet.

FTP

This category allows you to configure various protections related to the FTP protocol. It includes the following:

- ***Block Known Ports*** on page 487
- ***Block Port Overflow*** on page 488
- ***Blocked FTP Commands*** on page 489
- ***FTP Bounce*** on page 486

FTP Bounce

When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.

You can configure how FTP bounce attacks should be handled.

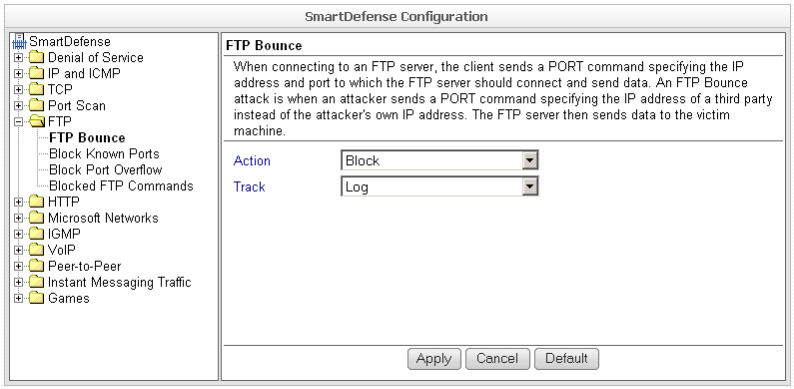

SmartDefense Configuration
SmartDefense
Denial of Service
IP and ICMP
TCP
Port Scan
FTP
FTP Bounce
Block Known Ports
Block Port Overflow
Blocked FTP Commands
HTTP
Microsoft Networks
IGMP
VoIP
Peer-to-Peer
Instant Messaging Traffic
Games
FTP Bounce
When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.
Action
Block
Track
Log
Apply
Cancel
Default

Table 99: FTP Bounce Fields

In this field…	Do this…
Action	Specify what action to take when an FTP Bounce attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log FTP Bounce attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Block Known Ports

You can choose to block the FTP server from connecting to well-known ports.

Note: Known ports are published ports associated with services (for example, SMTP is port 25).

This provides a second layer of protection against FTP bounce attacks, by preventing such attacks from reaching well-known ports.

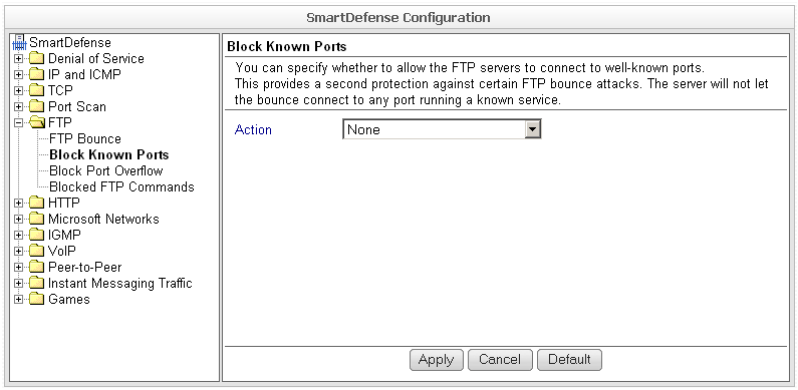


Table 100: Block Known Ports Fields

In this field…	Do this…
Action	Specify what action to take when the FTP server attempts to connect to a well-known port, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.

Block Port Overflow

FTP clients send PORT commands when connecting to the FTP sever. A PORT command consists of a series of numbers between 0 and 255, separated by commas.

To enforce compliance to the FTP standard and prevent potential attacks against the FTP server, you can block PORT commands that contain a number greater than 255.

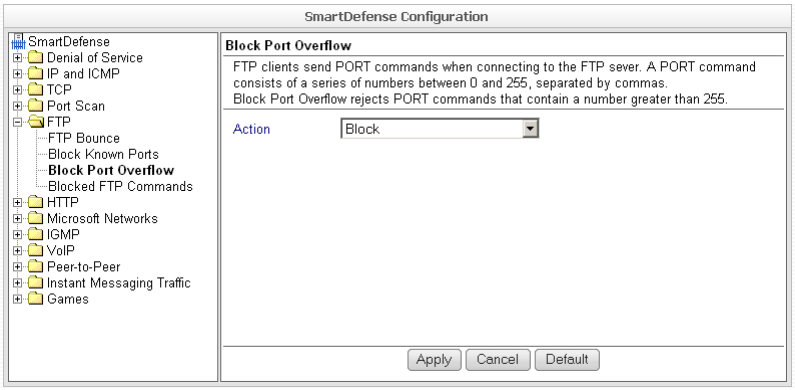
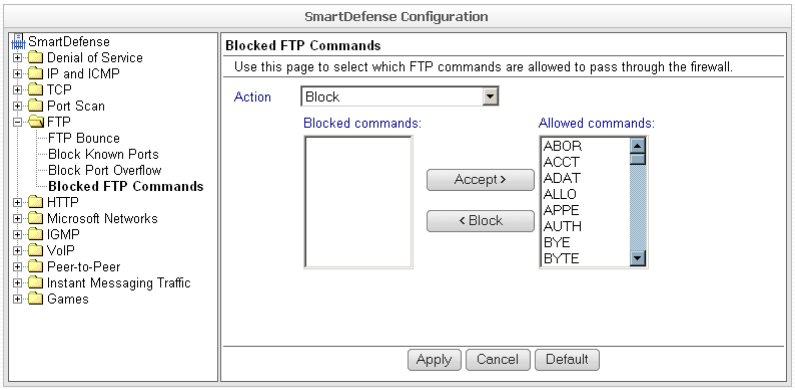


Table 101: Block Port Overflow

In this field...	Do this...
Action	Specify what action to take for PORT commands containing a number greater than 255, by selecting one of the following: • Block. Block the PORT command. This is the default. • None. No action.

Blocked FTP Commands

Some seldom-used FTP commands may compromise FTP server security and integrity. You can specify which FTP commands should be allowed to pass through the security server, and which should be blocked.



To enable FTP command blocking

- In the Action drop-down list, select Block.

  The FTP commands listed in the Blocked Commands box will be blocked.

  FTP command blocking is enabled by default.

To disable FTP command blocking

- In the Action drop-down list, select None.

  All FTP commands are allowed, including those in the Blocked Commands box.

To block a specific FTP command

1. In the Allowed Commands box, select the desired FTP command.
2. Click Block.

   The FTP command appears in the Blocked Commands box.
3. Click Apply.

   When FTP command blocking is enabled, the FTP command will be blocked.

To allow a specific FTP command

1. In the Blocked Commands box, select the desired FTP command.
2. Click Accept.

   The FTP command appears in the Allowed Commands box.
3. Click Apply.

   The FTP command will be allowed, regardless of whether FTP command blocking is enabled or disabled.

HTTP

This category allows you to configure various protections related to the HTTP protocol. It includes the following:

- ***Header Rejection*** on page 490
- ***Worm Catcher*** on page 491

Header Rejection

Some exploits are carried in standard HTTP headers with custom values (for example, in the Host header), or in custom HTTP headers. You can protect against such exploits by rejecting HTTP requests that contain specific headers and header values.

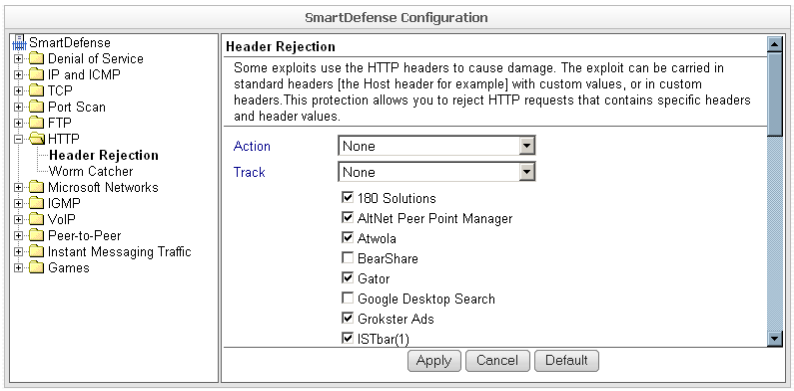


Table 102: Header Rejection Fields

In this field...	Do this...
Action	Specify what action to take when an HTTP header-based exploit is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP header-based exploits, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP header values list	Select the HTTP header values to detect.

Worm Catcher

A worm is a self-replicating malware (malicious software) that propagates by actively sending itself to new machines. Some worms propagate by using security vulnerabilities in the HTTP protocol.

You can specify how HTTP-based worm attacks should be handled.

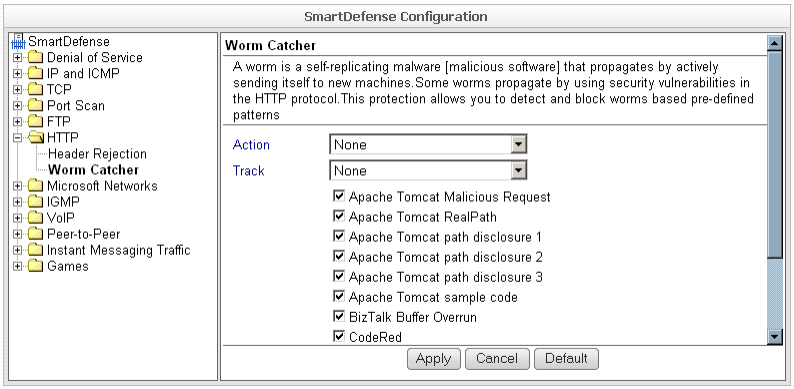


Table 103: Worm Catcher Fields

In this field…	Do this…
Action	Specify what action to take when an HTTP-based worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP-based worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP-based worm patterns list	Select the worm patterns to detect.

Microsoft Networks

This category includes File and Print Sharing.

Microsoft operating systems and Samba clients rely on Common Internet File System (CIFS), a protocol for sharing files and printers. However, this protocol is also widely used by worms as a means of propagation.

You can configure how CIFS worms should be handled.

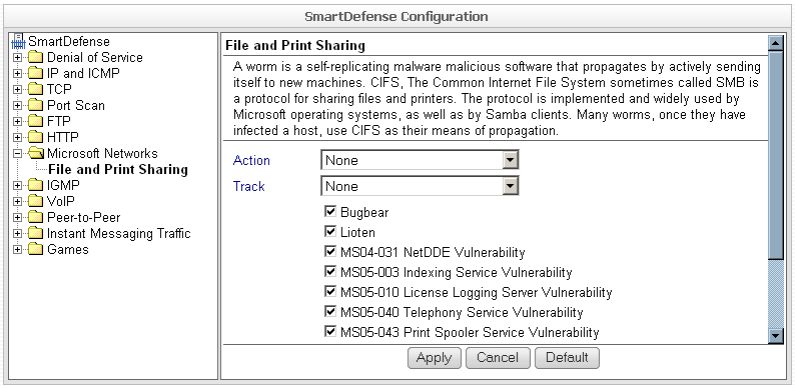

SmartDefense Configuration
SmartDefense
Denial of Service
IP and ICMP
TCP
Port Scan
FTP
HTTP
Microsoft Networks
File and Print Sharing
IGMP
VoIP
Peer-to-Peer
Instant Messaging Traffic
Games
File and Print Sharing
A worm is a self-replicating malware malicious software that propagates by actively sending itself to new machines. CIFS, The Common Internet File System sometimes called SMB is a protocol for sharing files and printers. The protocol is implemented and widely used by Microsoft operating systems, as well as by Samba clients. Many worms, once they have infected a host, use CIFS as their means of propagation.
Action
None
Track
None
Bugbear
Lioten
MS04-031 NetDDE Vulnerability
MS05-003 Indexing Service Vulnerability
MS05-010 License Logging Server Vulnerability
MS05-040 Telephony Service Vulnerability
MS05-043 Print Spooler Service Vulnerability
Apply
Cancel
Default

Table 104: File Print and Sharing Fields

In this field…	Do this…
Action	Specify what action to take when a CIFS worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log CIFS worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
CIFS worm patterns list	Select the worm patterns to detect. Patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server.

IGMP

This category includes the IGMP protocol.

IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

You can configure how IGMP attacks should be handled.

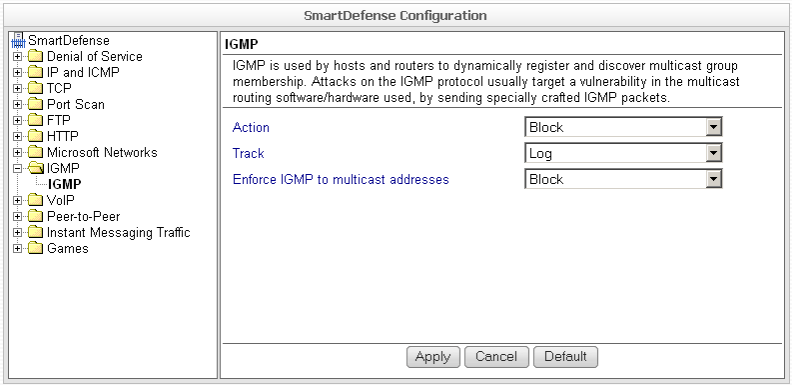


Table 105: IGMP Fields

In this field…	Do this…
Action	Specify what action to take when an IGMP attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log IGMP attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.
Enforce IGMP to multicast addresses	According to the IGMP specification, IGMP packets must be sent to multicast addresses. Sending IGMP packets to a unicast or broadcast address might constitute and attack; therefore the Safe@Office appliance blocks such packets.

In this field...	Do this...
	Specify whether to allow or block IGMP packets that are sent to non-multicast addresses, by selecting one of the following: • Block. Block IGMP packets that are sent to non-multicast addresses. This is the default. • None. No action.

VoIP

Voice over IP (VoIP) traffic is subject to various threats, such as:

- Call redirections, in which calls intended for one recipient are redirected to another
- Stealing calls, where the caller pretends to be someone else
- System hacking, using ports that were opened for VoIP connections

This category allows you to configure various protections related to VoIP protocols. It includes the following:

- ***SIP*** on page 496
- ***H.323*** on page 497

SIP

The SmartDefense SIP Application Level Gateway (ALG) processes the SIP protocol, allows firewall and NAT traversal, and enables Traffic Shaper to operate on SIP connections.

By default, the SIP ALG checks SIP sessions for RFC compliance. If desired, you can allow non-RFC-compliant SIP connections, so that VoIP devices that initiate non-standard SIP calls can communicate through the firewall. You can also disable the SIP ALG altogether, if it is not needed by your SIP clients, or if it interferes with their operation.

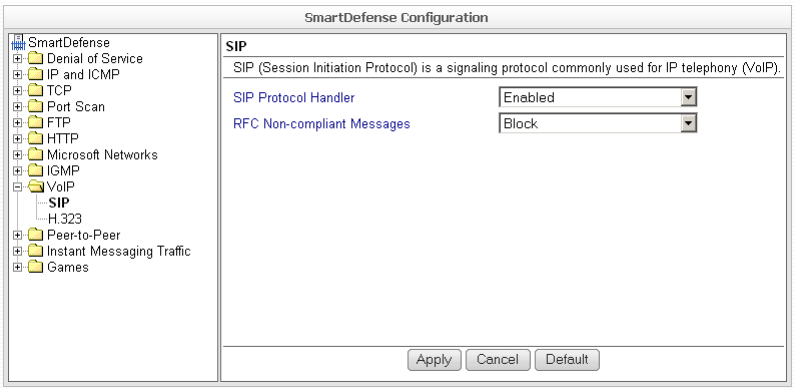


Table 106: SIP Fields

In this field...	Do this...
SIP Protocol Handler	Specify whether to enable SIP support, by selecting one of the following: • Enabled. Enable SIP support. This is the default. • Disabled. Disable SIP support.
RFC Non-compliant Messages	Specify what action to take when non-RFC-compliant SIP packets arrive, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.

H.323

H.323 telephony is used by various devices and applications, such as Microsoft Netmeeting. SmartDefense allows you to choose whether to disable or enable the H.323 Application Level Gateway (ALG), which allows firewall and NAT traversal of H.323 calls.

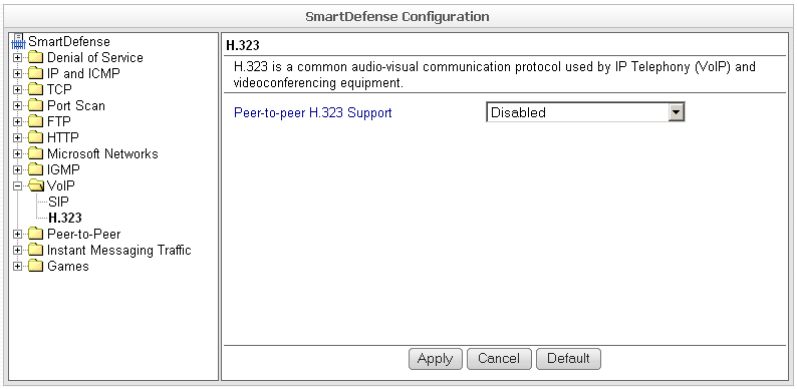


Table 107: H.323 Fields

In this field…	Do this…
Peer-to-peer H.323 Support	Specify whether to enable H.323 support, by selecting one of the following: • Enabled. Enable H.323 support. • Disabled. Disabled H.323 support. This is the default.

Peer-to-Peer

SmartDefense can block peer-to-peer file-sharing traffic, by identifying the proprietary protocols and preventing the initial connection to the peer-to-peer networks. This prevents not only downloads, but also search operations.

This category includes the following nodes:

- BitTorrent
- eMule
- Gnutella
- KaZaA
- Winny

Note: SmartDefense can detect peer-to-peer traffic regardless of the TCP port being used to initiate the session.

In each node, you can configure how peer-to-peer connections of the selected type should be handled, using the following table.

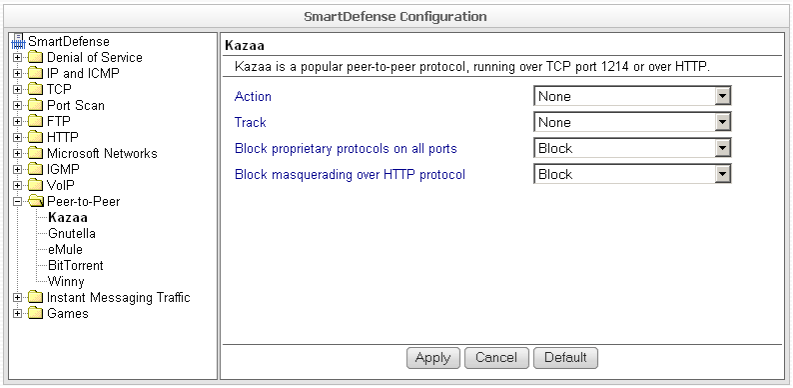


Table 108: Peer to Peer Fields

In this field...	Do this...
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log peer-to-peer connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.
Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this peer-to-peer application. This is the default. • None. Do not block the proprietary protocol on all ports.
Block masquerading over HTTP protocol	Specify whether to block using the peer-to-peer application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP. This field is not relevant for eMule and Winny.

Instant Messaging Traffic

SmartDefense can block instant messaging applications that use VoIP protocols, by identifying the messaging application's fingerprints and HTTP headers.

This category includes the following nodes:

- ICQ
- MSN Messenger
- Skype
- Yahoo

Note: SmartDefense can detect instant messaging traffic regardless of the TCP port being used to initiate the session.

Note: Skype versions up to 2.0.0.103 are supported.

In each node, you can configure how instant messaging connections of the selected type should be handled, using the following table.

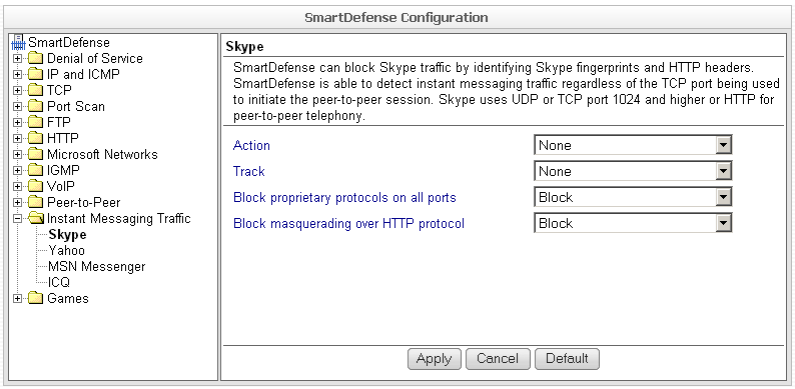


Table 109: Instant Messengers Fields

In this field…	Do this…
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log instant messenger connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.
Block proprietary protocol / Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this instant messenger application. This is the default. • None. Do not block the proprietary protocol on all ports.
Block masquerading over HTTP protocol	Specify whether to block using the instant messenger application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP.

Games

This category includes XBox LIVE.

XBox 360 requires gateways hosting XBox LIVE games to use the "Open NAT" method rather than the normal "Strict NAT" method. Therefore, if you want to host online games on an XBox 360 console, you must first configure your Safe@Office appliance to use the "Open NAT" method.

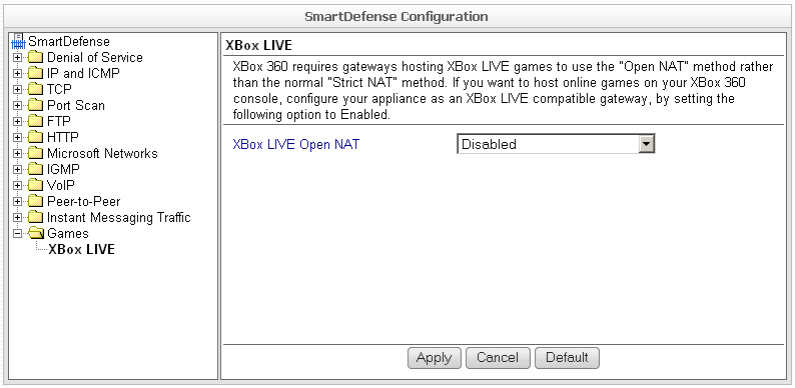


Table 110: XBox LIVE Fields

In this field...	Do this...
Xbox Live OpenNAT	Specify whether the Safe@Office appliance should use the "Open NAT" method, by selecting one of the following: • Enabled. Use the "Open NAT" method. You will be able to host XBox LIVE games and join existing ones. • Disabled. Do not use the "Open NAT" method. You will not be able to host XBox LIVE games, but you will still be able to join existing ones. This is the default.

Resetting SmartDefense to its Defaults

500 1000N

If desired, you can reset the SmartDefense security policy to its default settings. For information on the default value of each SmartDefense setting, see ***SmartDefense Categories*** on page 458.

For information on resetting individual nodes in the SmartDefense tree to their default settings, see ***Using the SmartDefense Tree*** on page 456.

To reset SmartDefense to its defaults

1. Click Security in the main menu, and click the SmartDefense tab.

   The SmartDefense page appears.

2. Click Reset to Defaults.

   A confirmation message appears.

3. Click OK.

   The SmartDefense policy is reset to its default settings.

Chapter 15

Using Antivirus and Antispam Filtering

This chapter explains how to use antivirus and antispam filtering.

This chapter includes the following topics:

Overview 505
Using VStream Antivirus 507
Using VStream Antispam 525
Using Centralized Email Filtering 558

Overview

The Safe@Office appliance enables you to perform both antivirus and antispam filtering, to ensure your network remains secure.

Antivirus Filtering Solutions

You can scan connections for viruses, by using VStream Antivirus and/or the Email Antivirus subscription service (part of the centralized Email Filtering service). The following table describes the main differences between VStream Antivirus and the Email Antivirus service:

Table 111: Comparison of Antivirus Filtering Methods

	VStream Antivirus	Email Antivirus
Supported Protocols	VStream Antivirus supports multiple protocols, including incoming SMTP and outgoing POP3 connections.	Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only.

	VStream Antivirus	Email Antivirus
Point of Enforcement	VStream Antivirus scans for viruses in the Safe@Office gateway itself.	Email Antivirus is centralized, redirecting traffic through the Service Center for scanning.

You can use either antivirus solution, or both in conjunction.

Antispam Filtering Solutions

You can scan email messages for spam, by using VStream Antispam and/or the Email Antispam subscription service (part of the centralized Email Filtering service). The following table describes the main differences between VStream Antispam and the Email Antispam service:

Table 112: Comparison of Antispam Filtering Methods

	VStream Antispam	Email Antispam
Supported Protocols	VStream Antispam supports both incoming and outgoing POP3 and SMTP, as well as POP3 and SMTP connections between internal networks.	Email Antispam scans incoming POP3 and outgoing SMTP connections only.
Point of Enforcement	VStream Antispam scans for spam in the Safe@Office gateway itself.	Email Antispam is centralized, redirecting traffic through the Service Center for scanning.

You can use either antispam solution, or both in conjunction.

Using VStream Antivirus

500 1000N

The Safe@Office appliance includes VStream Antivirus, an embedded stream-based antivirus engine based on Check Point Stateful Inspection and Application Intelligence technologies, that performs virus scanning at the kernel level.

VStream Antivirus scans files for malicious content on the fly, without downloading the files into intermediate storage. This means minimal added latency and support for unlimited file sizes; and since VStream Antivirus stores only minimal state information per connection, it can scan thousands of connections concurrently. In order to scan archive files on the fly, VStream Antivirus performs real-time decompression and scanning of ZIP, TAR, and GZ archive files, with support for nested archive files.

If you are subscribed to the VStream Antivirus subscription service, VStream Antivirus virus signatures are automatically updated, so that security is always up-to-date, and your network is always protected.

VStream Antivirus Actions

When VStream Antivirus detects malicious content, the action it takes depends on the protocol in which the virus was found. See the following table. In each case, VStream Antivirus blocks the file and writes a log to the Event Log.

Table 113: VStream Antivirus Actions

If a virus if found in this protocol...	VStream Antivirus does this...	The protocol is detected on this port...
HTTP	• Terminates the connection	All ports on which VStream Antivirus is enabled by the policy, not only port 80
POP3	• Terminates the connection • Deletes the virus-infected email from the server	The standard TCP port 110.

If a virus if found in this protocol...	VStream Antivirus does this...	The protocol is detected on this port...
IMAP	• Terminates the connection • Replaces the virus-infected email with a message notifying the user that a virus was found	The standard TCP port 143
SMTP	• Rejects the virus-infected email with error code 554 • Sends a "Virus detected" message to the sender	The standard TCP port 25
FTP	• Terminates the data connection • Sends a "Virus detected" message to the FTP client	The standard TCP port 21
TCP and UDP	• Terminates the connection	Generic TCP and UDP ports, other than those listed above

Note: In protocols that are not listed in this table, VStream Antivirus uses a "best effort" approach to detect viruses. In such cases, detection of viruses is not guaranteed and depends on the specific encoding used by the protocol.

Default Antivirus Policy

The VStream Antivirus default policy includes the following rules:

- All SMTP connections are scanned, regardless of the connection's direction.
- All POP3 connections are scanned, regardless of the connection's direction.
- All IMAP connections are scanned, regardless of the connection's direction.

You can easily override the default antivirus policy, by creating user-defined rules. For further information, see ***Configuring the VStream Antivirus Policy*** on page 511.

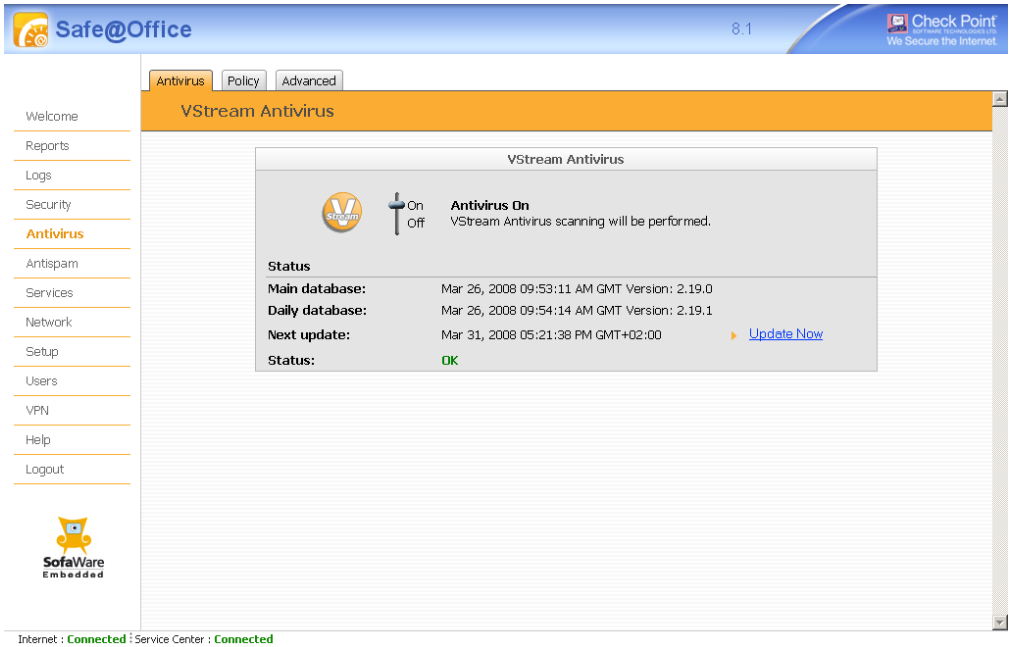
Enabling/Disabling VStream Antivirus

500 1000N

To enable/disable VStream Antivirus

1. Click Antivirus in the main menu, and click the Antivirus tab.

   The VStream Antivirus page appears.



2. Drag the On/Off lever upwards or downwards.

   VStream Antivirus is enabled/disabled for all internal network computers.

Viewing VStream Antivirus Signature Database Information

500 1000N

VStream Antivirus maintains two databases: a daily database and a main database. The daily database is updated frequently with the newest virus signatures. Periodically, the contents of the daily database are moved to the main database, leaving the daily database empty. This system of incremental updates to the main database allows for quicker updates and saves on network bandwidth.

You can view information about the VStream Antivirus signature databases currently in use, in the VStream Antivirus page.

Table 114: VStream Antivirus Page Fields

This field…	Displays…
Main database	The date and time at which the main database was last updated, followed by the version number.
Daily database	The date and time at which the daily database was last updated, followed by the version number.
Next update	The next date and time at which the Safe@Office appliance will check for updates.
Status	The current status of the database. This includes the following statuses: • Database Not Installed • OK

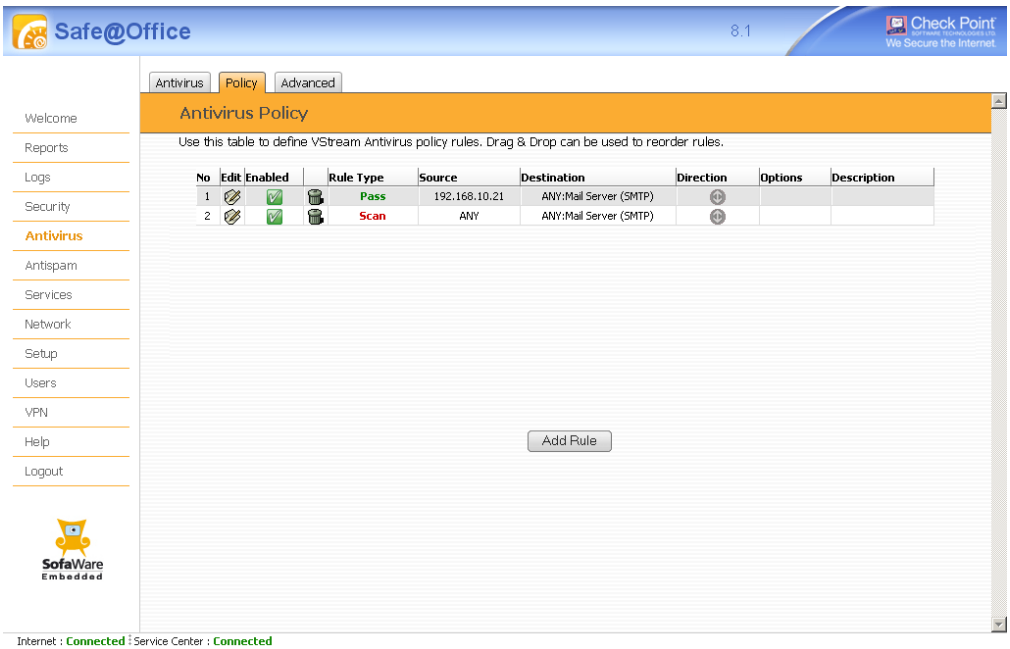
Configuring the VStream Antivirus Policy

500 1000N

VStream Antivirus includes a flexible mechanism that allows the user to define exactly which traffic should be scanned, by specifying the protocol, ports, and source and destination IP addresses.

VStream Antivirus processes policy rules in the order they appear in the Antivirus Policy table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to scan all outgoing SMTP traffic, except traffic from a specific IP address, you can create a rule scanning all outgoing SMTP traffic and move the rule down in the Antivirus Policy table. Then create a rule passing SMTP traffic from the desired IP address and move this rule to a higher location in the Antivirus Policy table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The Safe@Office appliance will process rule 1 first, passing outgoing SMTP traffic from the specified IP address, and only then it will process rule 2, scanning all outgoing SMTP traffic.

The following rule types exist:

Table 115: VStream Antivirus Rule Types

Rule	Description
Pass	This rule type enables you to specify that VStream Antivirus should not scan traffic matching the rule.
Scan	This rule type enables you to specify that VStream Antivirus should scan traffic matching the rule. If a virus is found, it is blocked and logged.

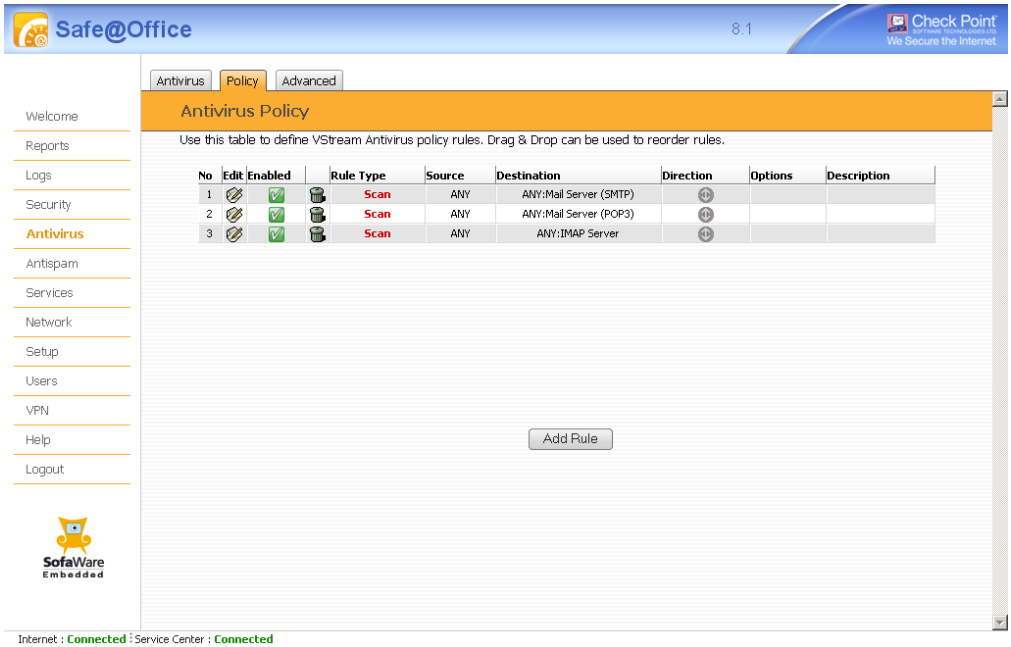
Adding and Editing VStream Antivirus Rules

500 1000N

To add or edit a VStream Antivirus rule

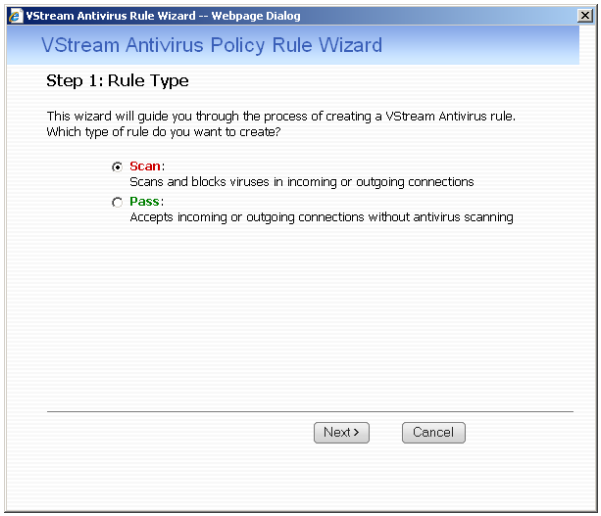
1. Click Antivirus in the main menu, and click the Policy tab.

The Antivirus Policy page appears.



2. Do one of the following:
   - To add a new rule, click Add Rule.
   - To edit an existing rule, click next to the desired rule.

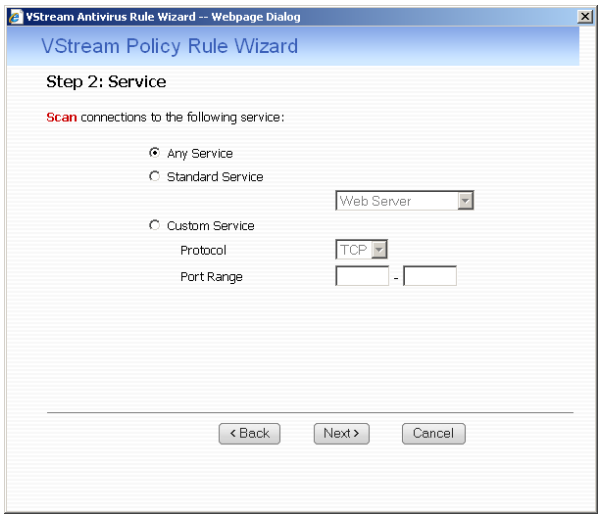
The VStream Policy Rule Wizard opens, with the Step 1: Rule Type dialog box displayed.


VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antivirus Policy Rule Wizard
Step 1: Rule Type
This wizard will guide you through the process of creating a VStream Antivirus rule.
Which type of rule do you want to create?
Scan:
Scans and blocks viruses in incoming or outgoing connections
Pass:
Accepts incoming or outgoing connections without antivirus scanning
Next >
Cancel

3. Select the type of rule you want to create.
4. Click Next.

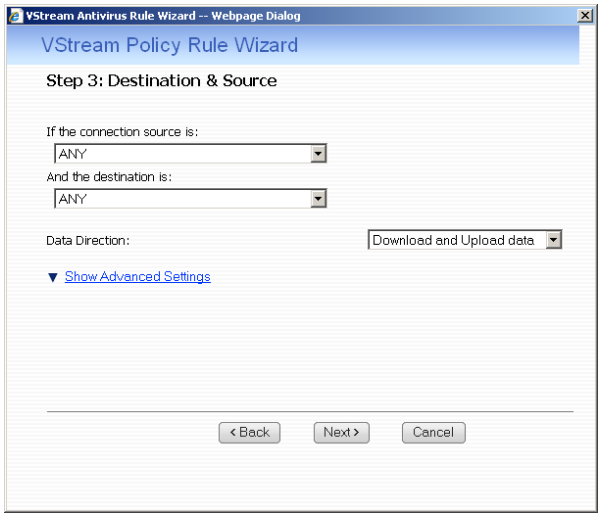
   The Step 2: Service dialog box appears.

   The example below shows a Scan rule.



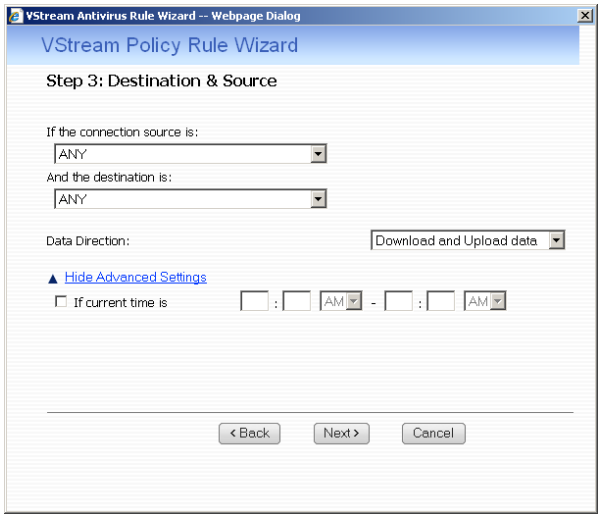
5. Complete the fields using the relevant information in the following table.
6. Click **Next**.

   The **Step 3: Destination & Source** dialog box appears.



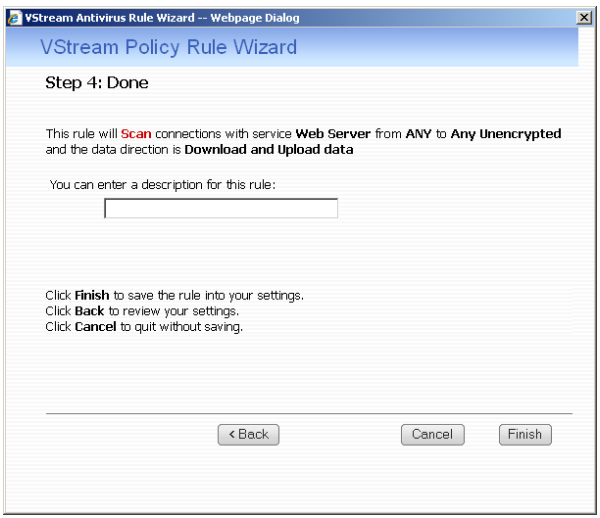
7. To configure advanced settings, click **Show Advanced Settings**.

   New fields appear.



8. Complete the fields using the relevant information in the following table.
9. Click Next.

   The Step 4: Done dialog box appears.


VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Policy Rule Wizard
Step 4: Done
This rule will Scan connections with service Web Server from ANY to Any Unencrypted and the data direction is Download and Upload data
You can enter a description for this rule:
Click Finish to save the rule into your settings.
Click Back to review your settings.
Click Cancel to quit without saving.
< Back
Cancel
Finish

10. If desired, type a description of the rule in the field provided.
11. Click Finish.

    The new rule appears in the Antivirus Policy page.

Table 116: VStream Antivirus Rule Fields

In this field...	Do this...
Any Service	Click this option to specify that the rule should apply to any service.
Standard Service	Click this option to specify that the rule should apply to a specific standard service or network service object. You must then select the desired service or network service object from the drop-down list.

In this field...	Do this...
Custom Service	Click this option to specify that the rule should apply to a specific non-standard service. The Protocol and Port Range fields are enabled. You must fill them in.
Protocol	Select the protocol (TCP, UDP, or ANY) for which the rule should apply.
Port Range	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. Note: If you do not enter a port range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.
If the connection source is	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify any source, select ANY.
And the destination is	Select the destination of the connections you want to allow or block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.

In this field...	Do this...
Data Direction	Select the direction of connections to which the rule should apply: • **Download and Upload data**. The rule applies to downloaded and uploaded data. This is the default. • **Download data**. The rule applies to downloaded data, that is, data flowing from the destination of the connection to the source of the connection. • **Upload data**. The rule applies to uploaded data, that is, data flowing from the source of the connection to the destination of the connection.
If the current time is	Select this option to specify that the rule should be applied only during certain hours of the day. You must then use the fields and drop-down lists provided, to specify the desired time range.

Enabling/Disabling VStream Antivirus Rules

500

You can temporarily disable a VStream Antivirus rule.

To enable/disable a VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears.

2. Next to the desired rule, do one of the following:

   - To enable the rule, click .

     The button changes to and the rule is enabled.

   - To disable the rule, click .

     The button changes to and the rule is disabled.

Reordering VStream Antivirus Rules

500 1000N

To reorder VStream Antivirus rules

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Viewing and Deleting VStream Antivirus Rules

500 1000N

To view or delete an existing VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears with a list of existing VStream Antivirus rules.
2. To resize a column, drag the relevant column divider right or left.
3. To delete a rule, do the following.

   a. In the desired rule's row, click .
   A confirmation message appears.
   b. Click OK.
   The rule is deleted.

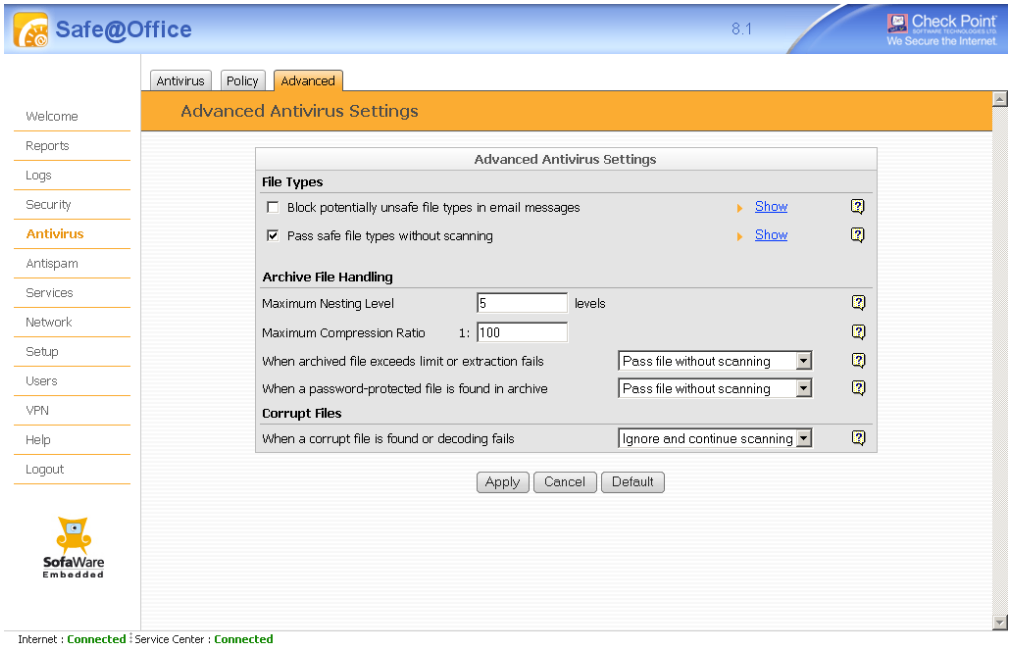
Configuring VStream Antivirus Advanced Settings

500 1000N

To configure VStream Antivirus advanced settings

1. Click Antivirus in the main menu, and click the Advanced tab.

The Advanced Antivirus Settings page appears.



2. Complete the fields using the following table.
3. Click Apply.
4. To restore the default VStream Antivirus settings, do the following:
   a) Click Default.

      A confirmation message appears.
   b) Click OK.

      The VStream Antivirus settings are reset to their defaults. For information on the default values, refer to the following table.

Table 117: Advanced Antivirus Settings Fields

In this field…	Do this…
File Types	
Block potentially unsafe file types in email messages	Select this option to block all emails containing potentially unsafe attachments. Unsafe file types are: • DOS/Windows executables, libraries and drivers • Compiled HTML Help files • VBScript encoded files • Files with {CLSID} in their name • The following file extensions: ade, adp, bas, bat, chm, cmd,com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs,shb, url, vb, vbe, vbs, wsc, wsf, wsh. To view a list of unsafe file types and their descriptions, click Show next to this option.
Pass safe file types without scanning	Select this option to accept common file types that are known to be safe, without scanning them. Safe files types are: • GIF • BMP • JFIF standard • EXIF standard • PNG • MPEG video stream • MPEG sys stream • Ogg Stream • MP3 file with ID3 version 2 • MP3 • PDF • PostScript

In this field...	Do this...
	• WMA/WMV/ASF • RealMedia file • JPEG - only the header is scanned, and the rest of the file is skipped To view a list of safe file types, click Show next to this option. Selecting this option reduces the load on the gateway by skipping safe file types. This option is selected by default.
Archive File Handling	
Maximum Nesting Level	Type the maximum number of nested content levels that VStream Antivirus should scan. Setting a higher number increases security. Setting a lower number prevents attackers from overloading the gateway by sending extremely nested archive files. The default value is 5 levels.
Maximum Compression Ratio 1:x	Fill in the field to complete the maximum compression ratio of files that VStream Antivirus should scan. For example, to specify a 1:80 maximum compression ratio, type 80. Setting a higher number allows the scanning of highly compressed files, but creates a potential for highly compressible files to create a heavy load on the appliance. Setting a lower number prevents attackers from overloading the gateway by sending extremely compressible files. The default value is 100.

In this field…	Do this…
When archived file exceeds limit or extraction fails	Specify how VStream Antivirus should handle files that exceed the Maximum nesting level or the Maximum compression ratio, and files for which scanning fails. Select one of the following: • Pass file without scanning. Scan only the number of levels specified, and skip the scanning of more deeply nested archives. Furthermore, skip scanning highly compressible files, and skip scanning archives that cannot be extracted because they are corrupt. This is the default. • Block file. Block the file.
When a password-protected file is found in archive	VStream Antivirus cannot extract and scan password-protected files inside archives. Specify how VStream Antivirus should handle such files, by selecting one of the following: • Pass file without scanning. Accept the file without scanning it. This is the default. • Block file. Block the file.
Corrupt Files	
When a corrupt file is found or decoding fails	Specify how VStream Antivirus should handle corrupt files and protocol anomalies, by selecting one of the following: • Ignore and continue scanning. Log the corrupt file or protocol anomaly, and scan the information on a best-effort basis. This is the default. • Block file. Block and log the corrupt file or protocol anomaly.

Updating VStream Antivirus

500 1000N

When you are subscribed to the VStream Antivirus updates service, VStream Antivirus virus signatures are automatically updated, keeping security up-to-date with no need for user intervention. However, you can still check for updates manually, if needed.

To update the VStream Antivirus virus signature database

1. Click Antivirus in the main menu, and click the Antivirus tab.

   The VStream Antivirus page appears.

2. Click Update Now.

   The VStream Antivirus database is updated with the latest virus signatures.

Using VStream Antispam

500 1000N

The Safe@Office appliance includes VStream Antispam, an embedded antispam engine that scans emails for spam. VStream Antispam is composed three antispam engines, each of which can be enabled or disabled separately:

- IP Reputation

  The IP Reputation engine protects mail servers by checking the email sender's IP address against an online and constantly updated IP reputation database, before accepting the SMTP email connection. If the IP address belongs to a known spammer, the connection can be immediately blocked at the TCP connection level, thereby stopping the spam before it reaches your mail server.

Note: If you have a mail server in your network, it is recommended to enable the IP Reputation engine as a first line of defense for incoming SMTP connections. When enabled, the IP Reputation engine blocks emails that would otherwise reach your mail server and require extensive analysis by the Content Based Antispam and Block List engines, both of which examine email content and consume network, gateway, and mail server resources. By reducing the amount of emails that require in-depth analysis, the IP Reputation engine helps prevent Denial of Service (DoS)

attacks on your gateway or mail server.

If you do not have a mail server in your network, there is no need to enable the IP Reputation engine. (If you do enable this engine anyway, it will have no negative effects.)

- Block List

  VStream Antispam allows configuring a list of senders whose emails should be blocked. When an email reaches your mail server, the Block List engine determines whether the sender's email address appears on the list. If so, then VStream Antispam blocks the emails.

- Content Based Antispam

  The Content Based Antispam engine calculates a “spam fingerprint” for each incoming email message. The fingerprint is then sent to a VStream Antispam data center and compared to a constantly updated database of spam messages. The data center returns a "spam score", which is a value in percentages indicating the likelihood that the message is spam. If the spam score exceeds a user-configurable threshold called the “confidence level”, the message can be flagged as spam, or the message can be deleted altogether.

In addition, VStream Antispam allows you to define a Safe Sender List, which consists of senders who are exempt from the Block List and Content Based Antispam engines.

The following table provides a comparison of the VStream Antispam engines.

Table 118: Comparison of VStream Antispam Engines

	IP Reputation	Content Based Antispam and Block List
Supported Protocols	Protects mail servers only, and applies to the SMTP protocol only	Protects both mail servers and mail clients, and applies to both POP3 and SMTP protocols
Email Scanning Time	Scans the email before accepting the connection	Scans the email after accepting the connection

	IP Reputation	Content Based Antispam and Block List
Detection Method	Examines the sender's IP address	Content Based Antispam examines the email's content, and Block List examines the email's Sender field.
SMTP Error Message	Does not return an SMTP error message to the email sender	Returns an SMTP error message to the email sender
Mail Rejection Method	Resets the TCP connection	Marks the email Subject line, marks the email header, rejects the email (SMTP only), or deletes the email (POP3 only)
Server Overload Protection	Prevents spammers from overloading gateway and mail server resources	Does not prevent spammers from overloading gateway and mail server resources

Important: In order to use VStream Antispam, your Safe@Office appliance must be subscribed to a Service Center.

How VStream Antispam Works

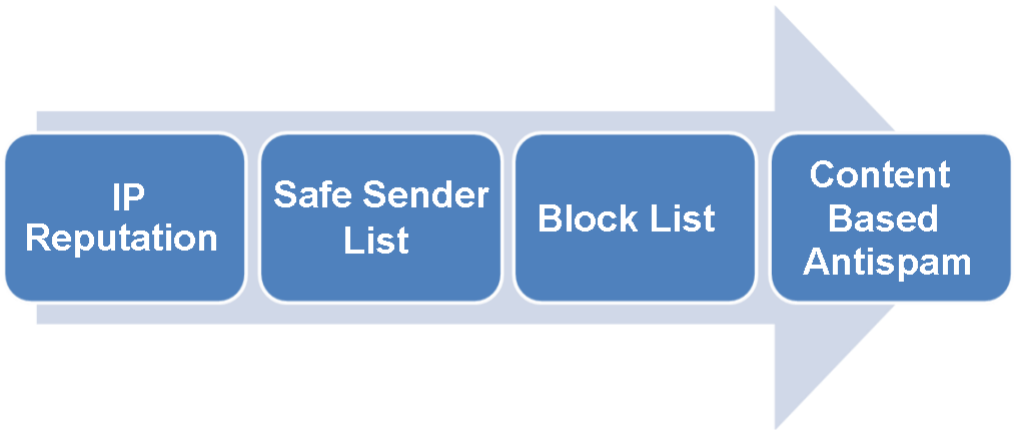


Figure 36: VStream Antispam Flow

VStream Antispam works as follows:

1. A TCP connection arrives at the SMTP port (TCP 25) or the POP3 port (TCP 110).
2. The connection is checked against the VStream Antispam policy, to determine whether it should be scanned.
3. If the IP Reputation engine is enabled, and the connection is an SMTP connection:
    a. VStream Antispam sends the connection's source IP address to a VStream Antispam data center.
    b. The VStream Antispam data center checks the reputation of this IP address against a list of known spam sender IP addresses, and then returns a spam score.
    c. One of the following things happens:
        - If the spam score does not exceed the configured confidence level, the email passes to the next enabled VStream Antispam engine for processing.

- If the spam score exceeds the configured confidence level, VStream Antispam determines that the email is spam and handles it as specified by the IP Reputation engine's settings.

d. VStream Antispam caches the results of the IP Reputation check.

4. VStream Antispam checks whether the email sender appears on the Safe Sender List. If so, then the email is accepted.
5. If the Block List engine is enabled:
   a. VStream Antispam examines the email content and compares the sender to the list of blocked senders.
   b. One of the following things happens:
      - If the sender is not on the list of blocked senders, the email passes to the next enabled VStream Antispam engine for processing.
      - If the sender is on the list of blocked senders, VStream Antispam determines that the email is spam and handles it as specified by the Block List engine's settings.

        By default, VStream Antispam marks the email subject.
6. If the Content Based Antispam engine is enabled:
   a. VStream Antispam examines the email content and creates a spam fingerprint.
   b. VStream Antispam sends the fingerprint to a VStream Antispam data center, where it is checked against an online database of spam messages.
   c. The VStream Antispam data center returns a spam score.
   d. One of the following things happens:
      - If the spam score does not exceed the configured confidence level, the email is accepted.
      - If the spam score exceeds the configured confidence level, VStream Antispam determines that email is spam and handles it and handles it as specified by the Content Based Antispam engine's settings.

        By default, VStream Antispam marks the email as spam.
7. One of the following things happen:
   - If the connection is an SMTP connection, the mail server forwards the email to the recipient.
   - If the connection is a POP3 connection, the email client receives the email.

Header Marking

VStream Antispam adds the following headers to each email that is scanned by the Content Based Antispam or Block List engine, but not blocked:

- `X-VStream-Spam-Level`. Contains an integer between 0 and 100, where 100 indicates the highest likelihood that the email is spam.
- `X-VStream-Engine`. The VStream Antispam engine, (either "Content Based Antispam" or "Block List")
- `X-Spam-Level`. Contains one to five asterisks, where five asterisks indicates the highest likelihood that the email is spam.
- `X-Spam-Flag`. Contains `YES` if the email is deemed to be spam, according to the currently configured thresholds.

For example:

```
X-VStream-Spam-Level: 81%
X-VStream-Engine: Content Based Antispam
X-Spam-Level: ***
X-Spam-Flag: YES
```

If your email client allows defining rules based on message headers, you can create rules specifying that emails with certain headers should be moved to specific folders. For example, you can configure your email client to move all emails with the `X-Spam-Flag: YES` header directly to a "Spam Email" folder.

Default Antispam Policy

The VStream Antispam default policy includes the following rules:

- All incoming SMTP connections are scanned, unless they originate from VPN. This protects mail servers in your network.
- All outgoing POP3 connections are scanned. This protects mail clients in your network.

You can easily override the default antispam policy, for example to exclude certain addresses or networks from spam scanning, by creating user-defined rules. For further information, see ***Configuring the VStream Antispam Policy*** on page 547.

Enabling/Disabling VStream Antispam

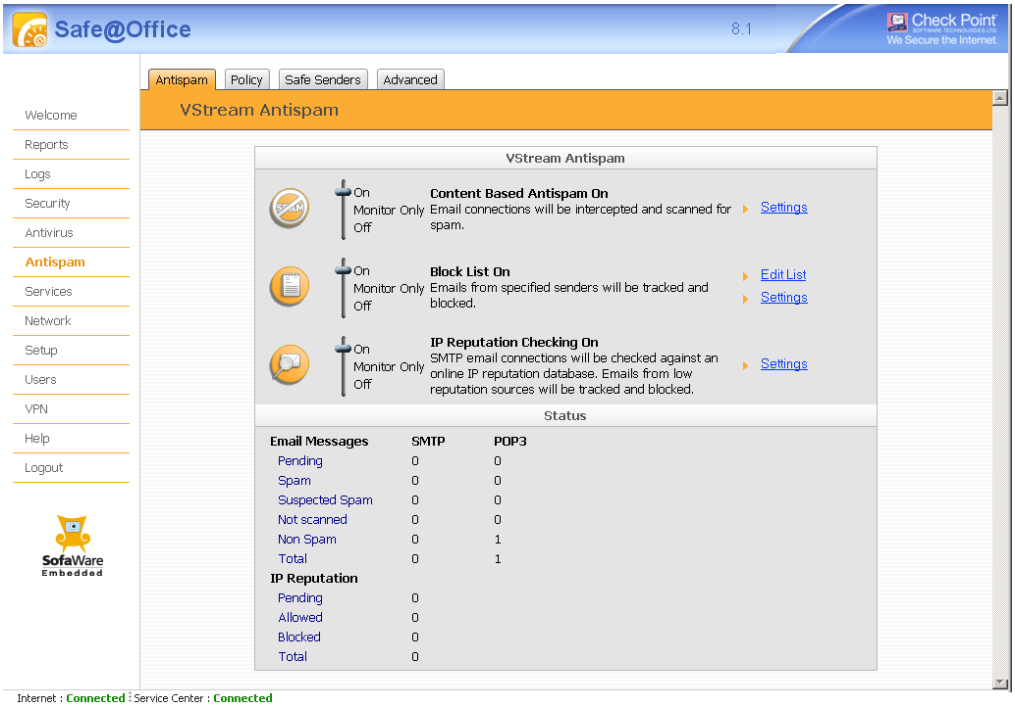
500 1000N

You must enable *at least one* VStream Antispam engine in order for VStream Antispam to work. Once you have enabled the desired engines, you must configure them, using the relevant sections in this guide.

To enable/disable VStream Antispam

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.



2. Complete the fields using the information in the following table.

Table 119: VStream Antispam Fields

In this field...	Do this...
Content Based Antispam	Specify the Content Based Antispam engine's mode, by dragging the lever to one of the following: • On. The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be handled according to configured Content Based Antispam settings. • Monitor Only. The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be *logged only*, and any action configured in the Content Based Antispam Settings page will *not* be performed. • Off. The Content Based Antispam engine is off. You can then click Settings to configure the Content Based Antispam settings. For further information, see ***Configuring the Content Based Antispam Engine*** on page 535.
Block List	Specify the Block List engine's mode, by dragging the lever to one of the following: • On. The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will be handled according to configured Block List settings. • Monitor Only. The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will be *logged only*, and any action configured in the Antispam Block List Settings page will *not* be performed. • Off. The Block List engine is off. You can then click Settings to configure the Block List settings. For further information, see ***Configuring the Block List Engine Settings*** on page 541.

In this field…	Do this…
IP Reputation Checking	Specify the IP Reputation engine's mode for SMTP connections, by dragging the lever to one of the following: • On. The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database prior to accepting the TCP connection. Emails that fail the check will be handled according to configured IP Reputation settings. • Monitor Only. The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database. Emails that fail the check will be *logged only*, and any action configured in the Antispam IP Reputation Settings page will *not* be performed. • Off. The IP Reputation engine is off. You can then click Settings to configure the IP Reputation settings. For further information, see ***Configuring the IP Reputation Engine*** on page 544.

Viewing VStream Antispam Statistics

To view VStream Antispam statistics

- Click Antispam in the main menu, and click the Antispam tab.

  The VStream Antispam page appears.

Table 120: VStream Antispam Status Fields

This field…	Displays…
Email Messages	Statistics for the Content Based Antispam and Block List engines.
Pending	The number of SMTP and POP3 email messages pending for the Content Based Antispam and Block List engines.

This field...	Displays...
Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be spam.
Suspected Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be suspected spam.
Not scanned	The number of SMTP and POP3 email messages that were not scanned, due to temporary loss of contact with the VStream Antispam data center, or due to gateway resource overload.
Non Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be legitimate.
Total	The total number of SMTP and POP3 email messages scanned by the Content Based Antispam and Block List engines.
IP Reputation	Statistics for the IP Reputation engine.
Pending	The number of SMTP email connections currently pending for handling by the IP Reputation engine.
Allowed	The number of SMTP email connections allowed by the IP Reputation engine.
Blocked	The number of SMTP email connections blocked by the IP Reputation engine.
Total	The total number of SMTP email connections scanned by the IP Reputation engine.

Configuring the Content Based Antispam Engine

500 1000N

You can configure how VStream Antispam should handle spam and suspected spam that is detected by the Content Based Antispam engine.

For information on enabling this engine, see ***Enabling/Disabling VStream Antispam*** on page 531.

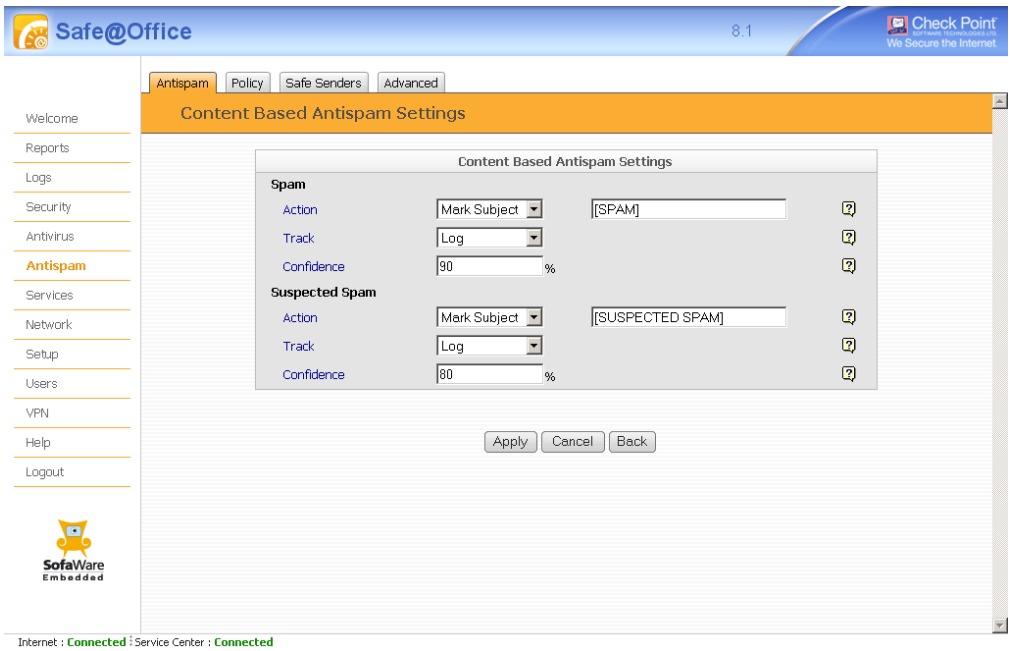
To configure Content Based Antispam engine settings

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the Content Based Antispam lever, click Settings.

   The Content Based Antispam Settings page appears.



3. Complete the fields using the information in the following table.

4. Click Apply.

Table 121: Content Based Antispam Settings Fields

In this field...	Do this...
Spam	Configure how VStream Antispam should handle spam that is detected using the Content Based Antispam engine.
Action	Specify the action VStream Antispam should take upon detecting spam, by selecting one of the following: • None. Take no action. • Reject. Block the email. The email will be permanently deleted. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Content Based Antispam engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 531.
Mark Text	Type the prefix to the text appearing in the Subject field of the spam notification email. For example, if you type `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way". The default value is `[SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.

In this field...	Do this...
Track	Specify whether VStream Antispam should log spam, by selecting one of the following: • Log. VStream Antispam should log spam. • None. VStream Antispam should not log spam.
Confidence	Type the minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email. The default value is 90.
Suspected Spam	Configure how VStream Antispam should handle suspected spam that is detected using the Content Based Antispam engine.
Action	Specify the action VStream Antispam should take upon detecting potential spam, by selecting one of the following: • None. Take no action. • Reject. Block the email. The email will be permanently deleted. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Content Based Antispam engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 531.
Mark Text	Type the prefix to the text appearing in the Subject field of the suspected spam notification email. For example, if you type `[SUSPECTED SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the suspected spam notification email's Subject field will display: "[SUSPECTED SPAM] Earn

In this field...	Do this...
	Money the Easy Way". The default value is `[SUSPECTED SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SUSPECTED SPAM]` directly to a Quarantine folder.
Track	Specify whether VStream Antispam should log suspected spam, by selecting one of the following: • Log. VStream Antispam should log suspected spam. • None. VStream Antispam should not log suspected spam.
Confidence	Type the minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered suspected spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email. The default value is 80.

Configuring the Block List Engine

500 1000N

You can configure a list of email addresses and domain names that VStream Antispam should automatically block, if the Block List engine is enabled.

For information on enabling the Block List engine, see ***Enabling/Disabling VStream Antispam*** on page 531.

Adding Blocked Senders

500 1000N

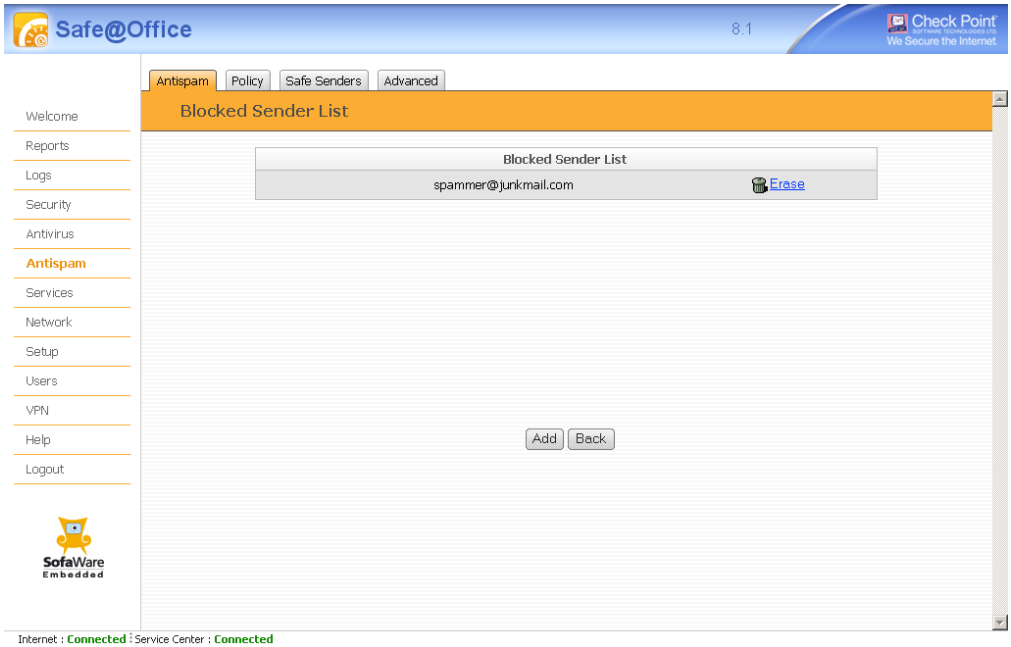
To add a blocked sender

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

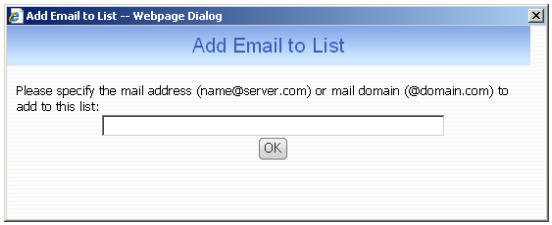
2. Next to the Block List lever, click Edit List.

The **Blocked Sender List** page appears.



3. Click **Add**.

   The **Add Email to List** dialog box appears.


Add Email to List -- Webpage Dialog
Add Email to List
Please specify the mail address (name@server.com) or mail domain (@domain.com) to add to this list:
OK

4. In the field provided, do one of the following:

   - To block all email from a specific sender, type the sender's email address.
   - To block all email from addresses ending with a specific domain, type the domain name.

     For example, if you type "@special-offers.com", then email addresses such as johns@special-offers.com and sarahm@special-offers.com will be blocked.

5. Click OK.

   The sender appears in the Block Sender List table.

Viewing and Deleting Blocked Senders

500 1000N

To delete a blocked sender

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the Block List lever, click Edit List.

   The Blocked Sender List page appears.

3. In the desired sender's row, click .

   The sender is deleted.

Configuring the Block List Engine Settings

500 1000N

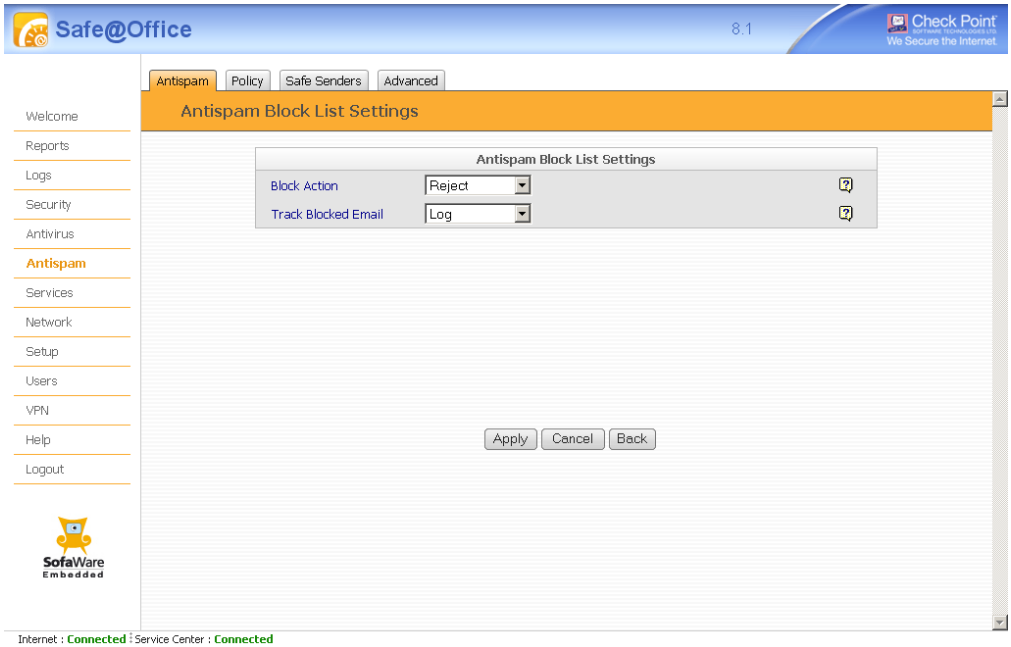
To configure Block List engine settings

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the Block List lever, click Settings.

The Antispam Block List Settings page appears.



3. Complete the fields using the information in the following table.
4. Click Apply.

Table 122: Antispam Block List Settings Fields

In this field...	Do this...
Block Action	Specify the action VStream Antispam should take upon receiving an email from a blocked sender, by selecting one of the following: • None. Take no action. • Reject. Block the email. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Block List engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 531.
Mark Text	Type the prefix to the text appearing in the Subject field of the spam notification email. For example, if you type `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way". The default value is `[SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.
Track Blocked Email	Specify whether VStream Antispam should log emails from blocked senders, by selecting one of the following: • Log. VStream Antispam should log emails from blocked senders. • None. VStream Antispam should not log emails from blocked senders.

Configuring the IP Reputation Engine

500 1000N

You can configure how VStream Antispam should handle spam and suspected spam that is detected by the IP Reputation engine.

For information on enabling this engine, see ***Enabling/Disabling VStream Antispam*** on page 531.

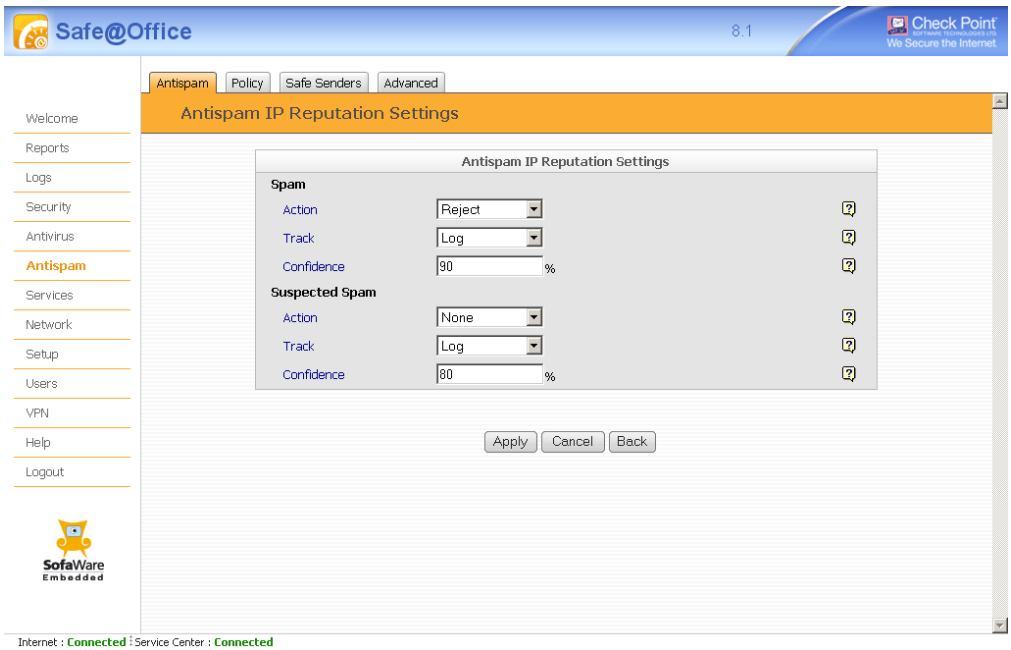
To configure IP Reputation engine settings

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the IP Reputation Checking lever, click Settings.

   The Antispam IP Reputation Settings page appears.



3. Complete the fields using the information in the following table.

4. Click Apply.

Table 123: Antispam IP Reputation Settings Fields

In this field…	Do this…
Spam	Configure how VStream Antispam should handle spam that is detected using the IP Reputation engine.
Action	Specify the action VStream Antispam should take upon detecting spam, by selecting one of the following: • Reject. Block the email. • None. Take no action. Note: If the IP Reputation engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 531.
Track	Specify whether VStream Antispam should log spam, by selecting one of the following: • Log. VStream Antispam should log spam. • None. VStream Antispam should not log spam.
Confidence	Type the minimum spam confidence level (SCL) needed to fail this check. If an email's SCL matches or exceeds this threshold, the email is considered spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email. The default value is 90.
Suspected Spam	Configure how VStream Antispam should handle suspected spam that is detected using the IP Reputation engine.

In this field...	Do this...
Action	Specify the action VStream Antispam should take upon detecting potential spam, by selecting one of the following: • Reject. Block the email. • None. Take no action. Note: If the IP Reputation engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 531.
Track	Specify whether VStream Antispam should log suspected spam, by selecting one of the following: • Log. VStream Antispam should log suspected spam. • None. VStream Antispam should not log suspected spam.
Confidence	Type the minimum spam confidence level (SCL) needed to fail this check. If an email's SCL matches or exceeds this threshold, the email is considered suspected spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email. The default value is 80.

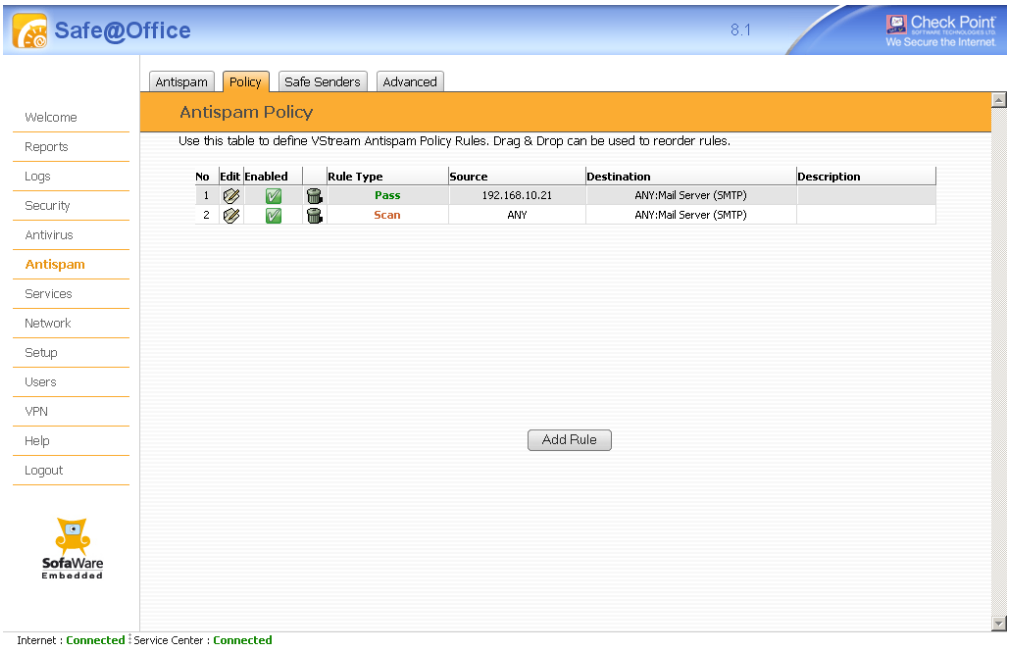
Configuring the VStream Antispam Policy

500 1000N

VStream Antispam includes a flexible mechanism that allows the user to define exactly which emails should be scanned for spam and which should be considered safe, by specifying the protocol, and the source and destination IP addresses.

VStream Antispam processes policy rules in the order they appear in the Antispam Policy table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to scan all outgoing SMTP traffic, except traffic from a specific IP address, you can create a rule scanning all outgoing SMTP traffic and move the rule down in the Antispam Policy table. Then create a rule passing SMTP traffic from the desired IP address and move this rule to a higher location in the Antispam Policy table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The Safe@Office appliance will process rule 1 first, passing outgoing SMTP traffic from the specified IP address, and only then it will process rule 2, scanning all outgoing SMTP traffic.

The following rule types exist:

Table 124: VStream Antispam Rule Types

Rule	Description
Pass	This rule type enables you to specify that VStream Antispam should allow all emails matching the rule, without scanning the emails.
Scan	This rule type enables you to specify that VStream Antispam should scan all emails matching the rule.
Reject	This rule type enables you to specify that VStream Antispam should reject all emails matching the rule, without scanning the emails.

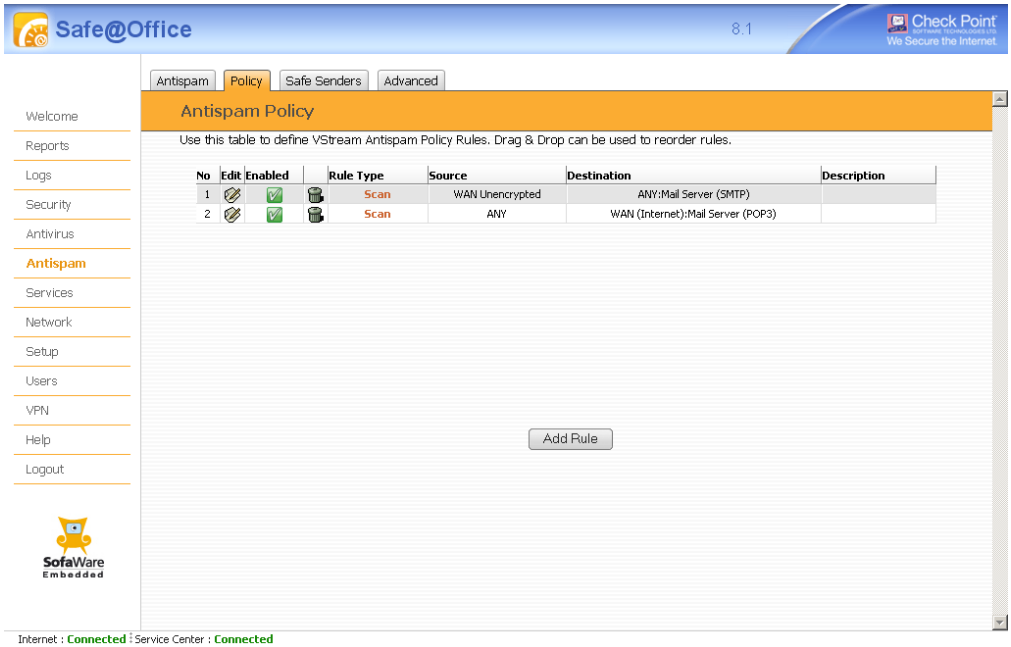
Adding and Editing VStream Antispam Rules

500 1000N

To add or edit a VStream Antispam rule

1. Click Antispam in the main menu, and click the Policy tab.

The **Antispam Policy** page appears.



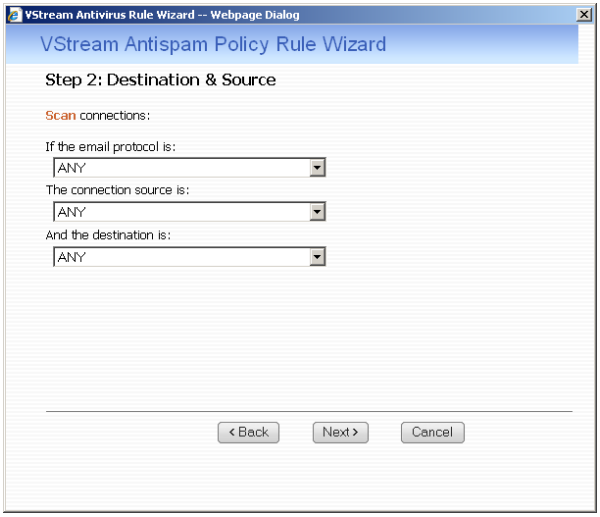
2. Do one of the following:
   - To add a new rule, click **Add Rule**.
   - To edit an existing rule, click next to the desired rule.

The VStream Antispam Policy Rule Wizard opens, with the Step 1: Rule Type dialog box displayed.

VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antispam Policy Rule Wizard
Step 1: Rule Type
This wizard will guide you through the process of creating a VStream Antispam rule.
Which type of rule do you want to create?
Scan:
Scans email messages for viruses and malicious content
Pass:
Immediately accepts emails from a certain source or destination, without antispam scanning
Reject:
Immediately rejects emails from a certain source or destination
Next >
Cancel

3. Select the type of rule you want to create.
4. Click Next.

   The Step 2: Destination & Source dialog box appears.



5. Complete the fields using the relevant information in the following table.

6. Click Next.

   The Step 3: Done dialog box appears.

VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antispam Policy Rule Wizard
Step 3: Done
This rule will Scan connections with service Web Server from ANY to ANY
You can enter a description for this rule:
Click Finish to save the rule.
Click Back to review your settings.
Click Cancel to quit without saving.
< Back
Cancel
Finish

7. If desired, type a description of the rule in the field provided.
8. Click Finish.

   The new rule appears in the Antispam Policy page.

Table 125: VStream Antispam Policy Rule Wizard Fields

In this field…	Do this…
If the email protocol is	Select the email protocol to which the rule should apply. The supported protocols are SMTP and POP3. To specify both SMTP and POP3, select ANY. Note: When defining a Reject rule, this field is set to Mail Server (SMTP).

In this field...	Do this...
The connection source is	Select the source of the connections to which the rule should apply. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify connections originating from this gateway, select This Gateway. To specify any source *except* this gateway, select ANY.
And the destination is	Select the destination of the connections to which the rule should apply. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
Description	Type a description of the rule.

Enabling/Disabling VStream Antispam Rules

500 1000N

You can temporarily disable a VStream Antispam rule.

To enable/disable a VStream Antispam rule

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears.

2. Next to the desired rule, do one of the following:

   - To enable the rule, click .

     The button changes to and the rule is enabled.

   - To disable the rule, click .

     The button changes to and the rule is disabled.

Reordering VStream Antispam Rules

500 1000N

To reorder VStream Antispam rules

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Viewing and Deleting VStream Antispam Rules

500 1000N

To view or delete an existing VStream Antispam rule

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears with a list of existing VStream Antispam rules.
2. To resize a column, drag the relevant column divider right or left.
3. To delete a rule, do the following.

   a. In the desired rule's row, click .
   A confirmation message appears.

   b. Click OK.
   The rule is deleted.

Configuring the Safe Sender List

500 1000N

You can configure a list of email addresses and domain names that are "safe". VStream Antispam will treat all emails sent from these addresses or domains as legitimate (non-spam) mail.

Note: The IP Reputation check is performed *before* accepting the TCP connection, at which point the sender's email address is not yet available. Therefore, if the IP Reputation engine is enabled, and an SMTP session is received from an IP address that is reputed to be a source of spam, VStream Antispam will block the connection, regardless of whether the sender's email address is on the Safe Sender List.

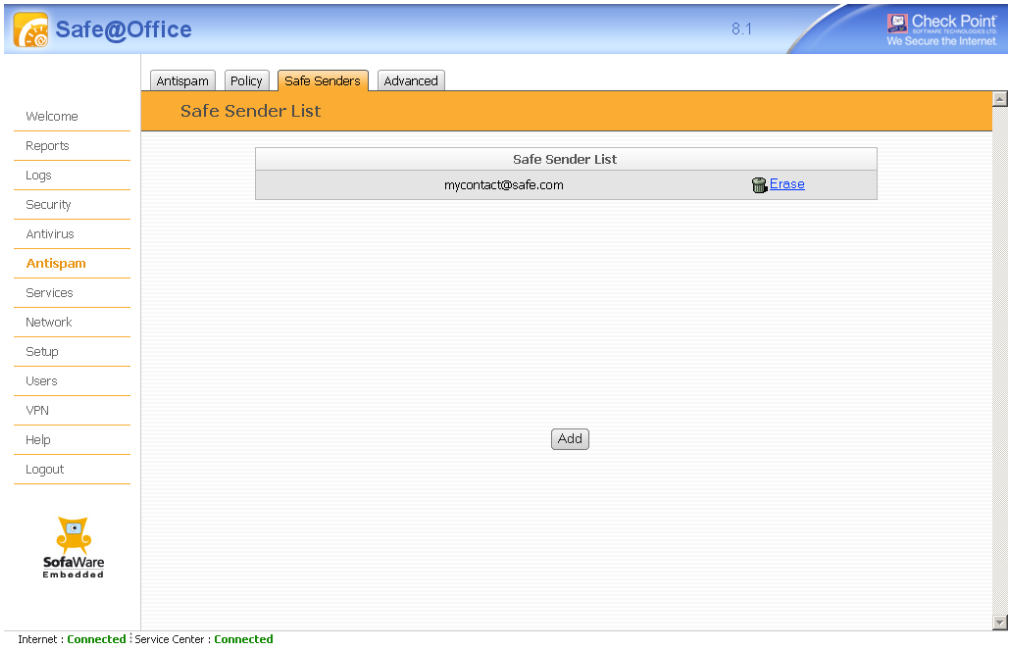
Adding Safe Senders

500 1000N

To add a safe sender

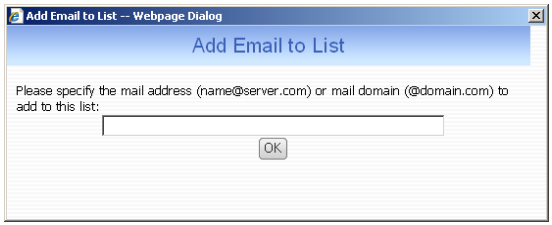
1. Click Antispam in the main menu, and click the Safe Senders tab.

The **Safe Sender List** page appears.



2. Click **Add**.

   The **Add Email to List** dialog box appears.


Add Email to List -- Webpage Dialog
Add Email to List
Please specify the mail address (name@server.com) or mail domain (@domain.com) to add to this list:
OK

3. In the field provided, do one of the following:

   - To allow all email from a specific sender, type the sender's email address.
   - To allow all email from addresses ending with a specific domain, type the domain name.

     For example, if you type "@mycompany.com", then email addresses such as johns@mycompany.com and sarahm@mycompany.com will be allowed.

4. Click OK.

   The sender appears in the Safe Senders table.

Viewing and Deleting Safe Senders

To view or delete a safe sender

1. Click Antispam in the main menu, and click the Safe Senders tab.

   The Safe Sender List page appears.

2. In the desired sender's row, click Erase.

   The sender is deleted.

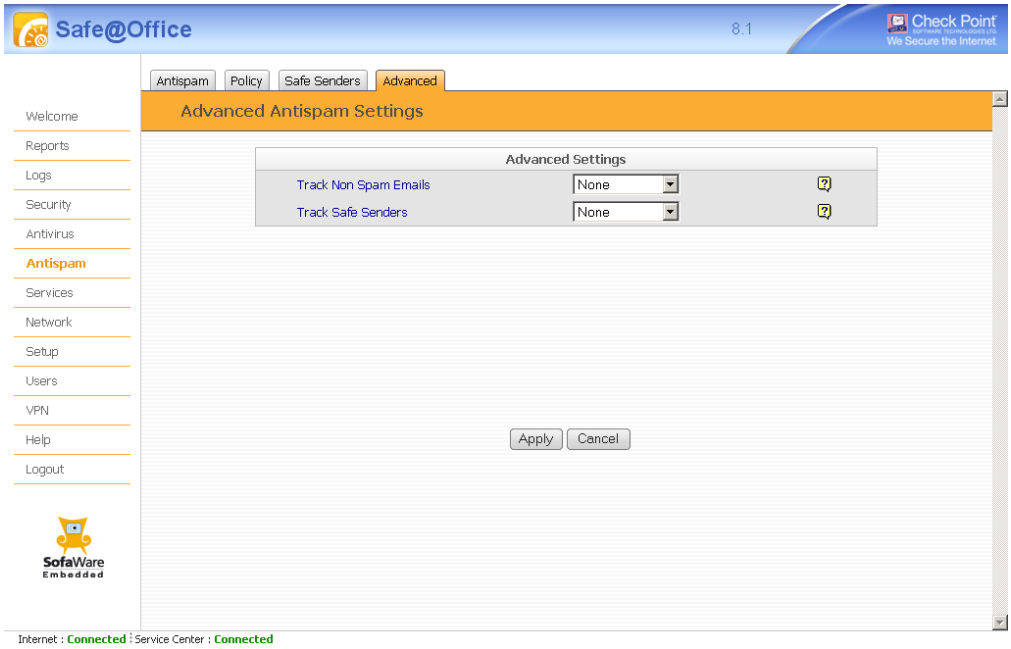
Configuring VStream Antispam Advanced Settings

500 1000N

To configure VStream Antispam advanced settings

1. Click Antispam in the main menu, and click the Advanced tab.

   The Advanced Antispam Settings page appears.



2. In the Track Non Spam Emails drop-down list, do one of the following:

   - To specify that VStream Antispam should log email that is detected as legitimate mail, select Log.
   - To specify that VStream Antivirus should not log email that is detected as legitimate mail, select None.

3. In the Track Safe Senders drop-down list, do one of the following:

   - To specify that VStream Antispam should log email sent by addresses on the Safe Sender List, select Log.

- To specify that VStream Antivirus should not log email sent by addresses on the Safe Sender List, select None.

4. Click Apply.

Using Centralized Email Filtering

500 1000N

There are two centralized Email Filtering services:

- Email Antivirus

  When the Email Antivirus service is enabled, your email is automatically scanned for the detection and elimination of all known viruses and vandals. If a virus is detected, it is removed and replaced with a warning message.

- Email Antispam

  When the Email Antispam service is enabled, your email is automatically scanned for the detection of spam. If spam is detected, the email's Subject line is modified to indicate that it is suspected spam. If your email client allows defining rules based on the Subject field, you can create rules to divert such messages to a special folder.

Note: Email Filtering services are only available if you are connected to a Service Center and subscribed to the services. For information on using subscription services, see ***Using Subscription Services*** on page *591*.

Note: For information on the differences between the centralized Email Filtering services and VStream Antivirus or VStream Antispam, see ***Overview*** on page *505*.

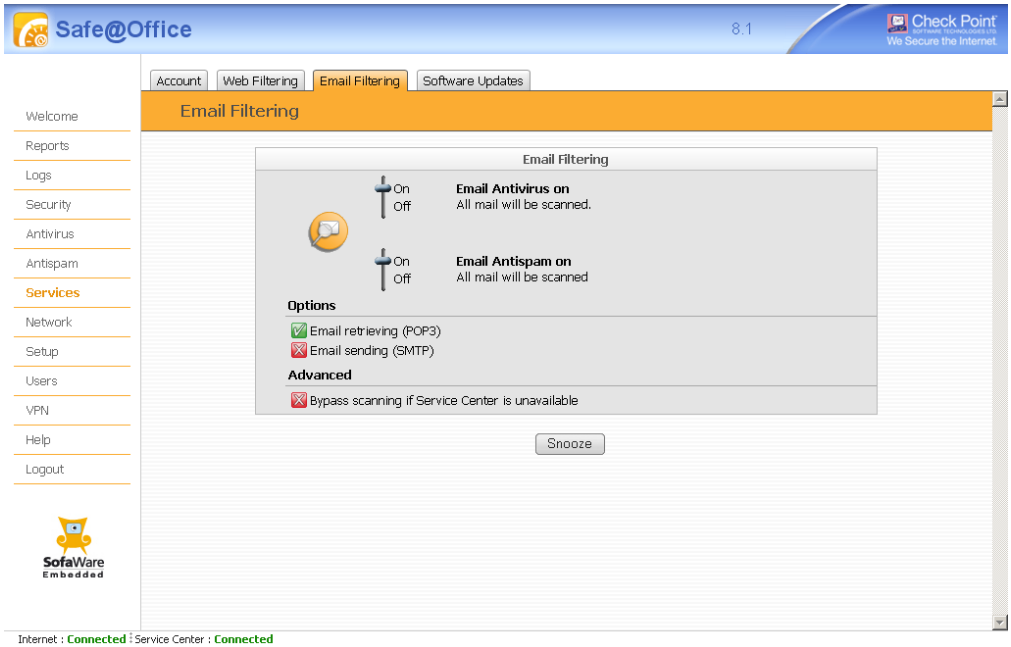
Enabling/Disabling Email Filtering

500 1000N

To enable/disable Email Filtering

1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.



2. Next to Email Antivirus, drag the On/Off lever upwards or downwards.

   Email Antivirus is enabled/disabled.

Selecting Protocols for Scanning

500 1000N

If you are locally managed, you can define which protocols should be scanned for viruses and spam:

- Email retrieving (POP3). If enabled, all incoming email in the POP3 protocol will be scanned.
- Email sending (SMTP). If enabled, all outgoing email will be scanned.

Protocols marked with ☑ will be scanned, while those marked with ☒ will not.

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To enable virus and spam scanning for a protocol

1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.

2. In the Options area, click ☑ or ☒ next to the desired protocol.

Configuring Email Filtering Advanced Settings

500 1000N

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To configure Email Filtering advanced settings

1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.

2. Next to the Bypass scanning if Service Center is unavailable option, specify how the gateway should handle Email Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all email traffic, click .

     This ensures constant protection from spam and viruses.

     The button changes to .

   - To temporarily allow all email traffic, click .

     This ensures continuous access to email; however, it does not protect against viruses and spam, so use this option cautiously.

     The button changes to .

   When the Service Center is available again, the gateway will enforce the configured Email Filtering policy.

Temporarily Disabling Email Filtering

500 1000N

If you are having problems sending or receiving email you can temporarily disable the Email Filtering services.

To temporarily disable Email Filtering

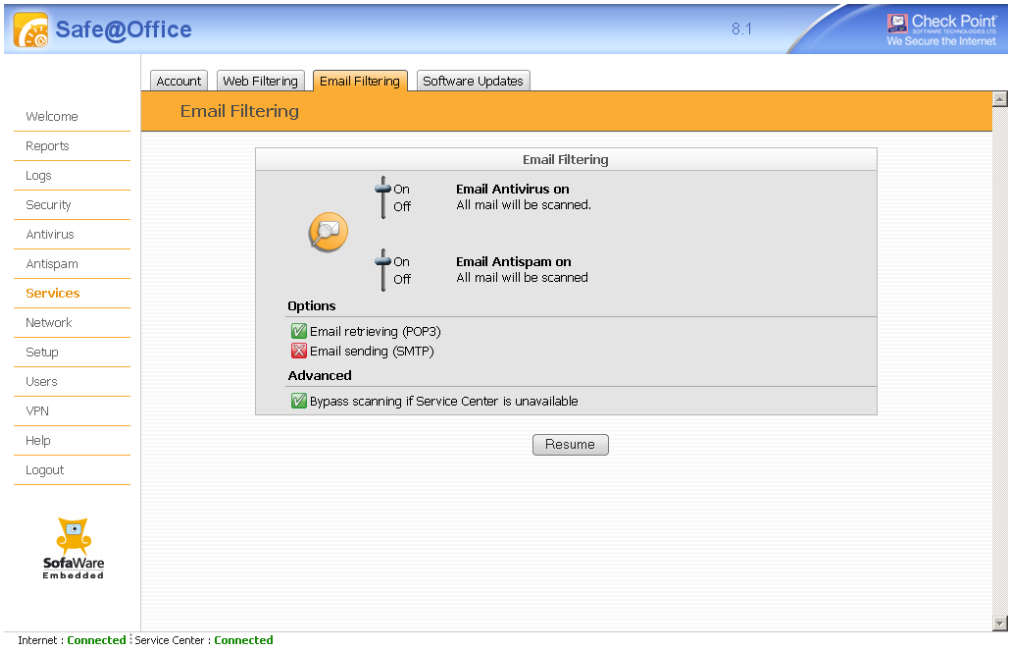
1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.

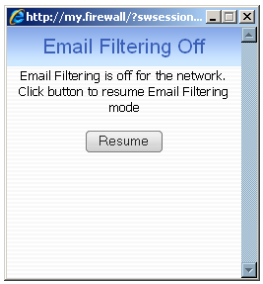
2. Click Snooze.

   - Email Antivirus and Email Antispam are temporarily disabled for all internal network computers.

- The Snooze button changes to Resume.



- The Email Filtering Off popup window opens.


http://my.firewall/?swsession...
Email Filtering Off
Email Filtering is off for the network. Click button to resume Email Filtering mode
Resume

3. To re-enable Email Antivirus and Email Antispam, click Resume, either in the popup window, or on the Email Filtering page.
   - The services are re-enabled for all internal network computers.
   - If you clicked Resume in the Email Filtering page, the button changes to Snooze.
   - If you clicked Resume in the Email Filtering Off popup window, the popup window closes.

Chapter 16

Using Web Content Filtering

This chapter explains how to use Web content filtering.

This chapter includes the following topics:

Overview 565
Using Web Rules 567
Using Web Filtering 575
Customizing the Access Denied Page 582

Overview

You can allow or block users from accessing Web content, by configuring Web rules and/or the Web Filtering service. The following table describes the main differences between Web rules and the Web Filtering service:

Table 126: Comparison of Web Content Filtering Methods

	Web Rules	Web Filtering
Filtering Action	Web rules allow and block specific URLs.	The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong.
Point of Enforcement	HTTP requests are analyzed in the gateway, by comparing each request against a list of rules.	HTTP requests are analyzed in the gateway, by extracting each request's URL and then sending the URL to the Service Center, to determine to which categories the URL belongs. The request is then allowed or denied according to the configured list of allowed categories.

	Web Rules	Web Filtering
Subscription and Connection Requirement	Web rules are included with the Safe@Office appliance and do not require a Service Center subscription or connection.	The Web Filtering service is subscription-based and requires a connection to the Service Center.

You can use either Web content filtering solution or both in conjunction. When a user attempts to access a Web site, the Safe@Office appliance first evaluates the Web rules. If the site is not blocked or allowed by the Web rules, the Web Filtering service is then consulted.

Regardless of which method is used, if a user attempts to access a blocked page, the Access Denied page appears. For information on customizing this page, see ***Customizing the Access Denied Page*** on page 582.

If desired, you can permit specific users to override Web content filtering, by granting them Web Filtering Override permissions. Such users will be able to view Web pages without restriction, after they have provided their username password via the Access Denied page. For information on granting Web Filtering Override permissions, see ***Adding and Editing Users*** on page 680.

In addition, you can choose to exclude specific network objects from Web content filtering enforcement. Users connecting from these network objects will be able to view Web pages without restriction, regardless of whether they have Web Filtering Override permissions. For information on configuring network objects, see ***Using Network Objects*** on page 227.

Using Web Rules

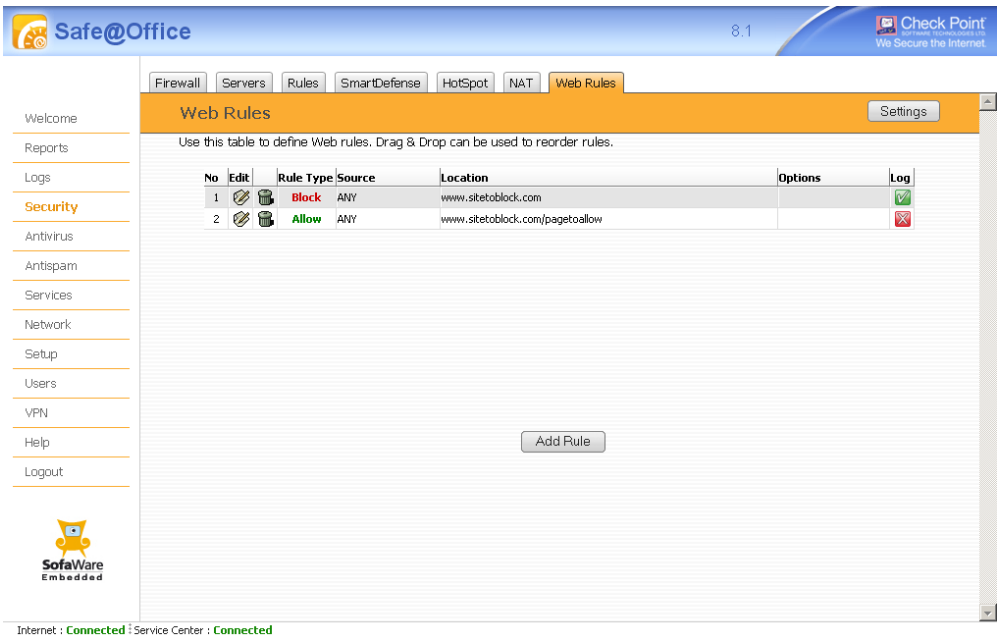
500 1000N

You can block or allow access to specific Web pages, by defining Web rules.

Note: Web rules affect outgoing traffic only and cannot be used to allow or limit access from the Internet to internal Web servers.

The Safe@Office appliance processes Web rules in the order they appear in the Web Rules table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Web Rules table.

For example, if you want to block all the pages of a particular Web site, except a specific page, you can create a rule blocking access to all of the Web site's pages and move the rule down in the Web Rules table. Then create a rule allowing access to the desired page and move this rule to a higher location in the Web Rules table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The Safe@Office appliance will process rule 1 first, allowing access to the desired page, and only then it will process rule 2, blocking access to the rest of the site.

The following rule types exist:

Table 127: Web Rule Types

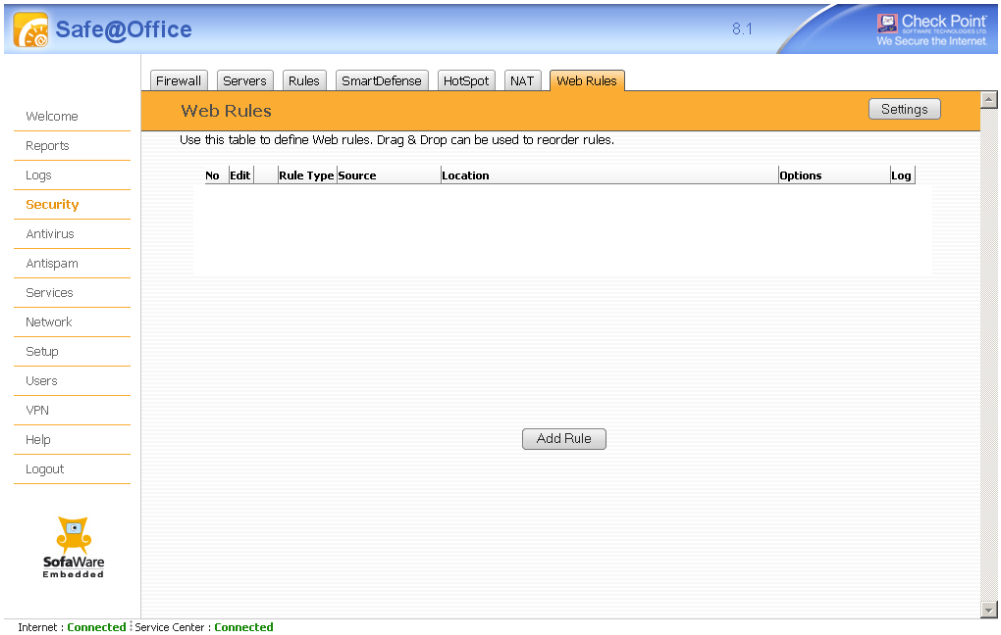
Rule	Description
Allow	This rule type enables you to specify that a specific Web page should be allowed.
Block	This rule type enables you to specify that a specific Web page should be blocked.

Adding and Editing Web Rules

To add or edit a Web rule

1. Click Security in the main menu, and click the Web Rules tab.

The **Web Rules** page appears.



2. Do one of the following:
   - To add a new rule, click **Add Rule**.
   - To edit an existing rule, click next to the desired rule.

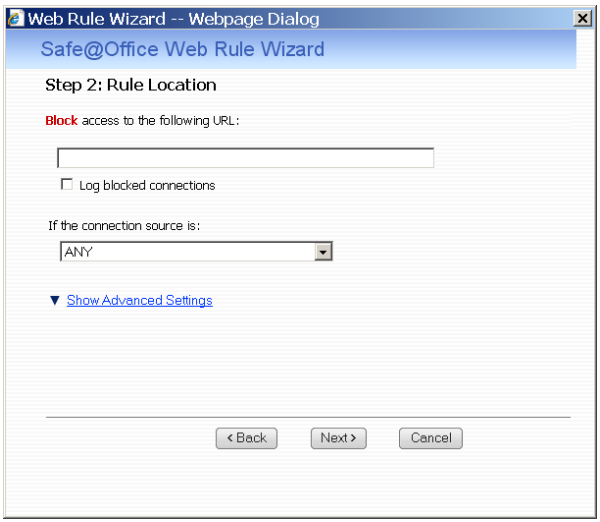
The Safe@Office Web Rule Wizard opens, with the Step 1: Rule Type dialog box displayed.

Web Rule Wizard -- Webpage Dialog
Safe@Office Web Rule Wizard
Step 1: Rule Type
This wizard will guide you through the process of creating a Web rule.
Which type of rule do you want to create?
Block:
Blocks users from accessing specified Web sites
Allow:
Allows users to access specified Web sites
Next >
Cancel

3. Select the type of rule you want to create.
4. Click Next.

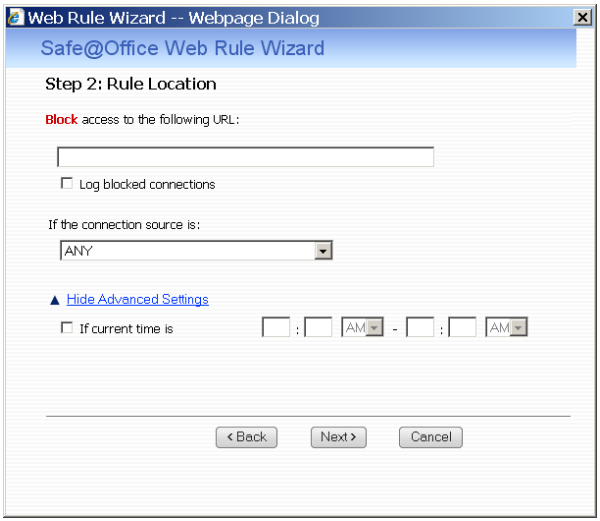
   The Step 2: Rule Location dialog box appears.

The example below shows a Block rule.



5. To configure advanced settings, click **Show Advanced Settings**.

   New fields appear.



6. Complete the fields using the relevant information in the following table.
7. Click **Next**.

The Step 3: Confirm Rule dialog box appears.

Web Rule Wizard -- Webpage Dialog
Safe@Office Web Rule Wizard
Step 3: Confirm Rule
This rule will Block and log access to the following URL www.sitetoblock.com from ANY.
Click Finish to save the rule into your settings.
Click Back to review your settings.
Click Cancel to quit without saving.
< Back
Cancel
Finish

8. Click Finish.

   The new rule appears in the Web Rules page.

Table 128: Web Rules Fields

In this field...	Do this...
Block/Allow access to the following URL	Type the URL or IP address to which the rule should apply. Wildcards (*) are supported. For example, to block all URLs that start with "http://www.casino-", set this field's value to: `http://www.casino-*` Note: If you block a Web site based on its domain name (http://<domain_name>), the Web site is not automatically blocked when surfing to the Web server's IP address (http://<IP_address>). Likewise, if you block a Web site based on its IP address, the Web site is not automatically blocked when surfing to the domain name. To prevent access to both the domain name and the IP address, you must block both.

In this field…	Do this…
Log allowed connections / Log blocked connections	Select this option to log the specified blocked or allowed connections. By default, allowed Web pages are not logged, and blocked Web pages are logged.
If the connection source is	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.
If the current time is	Select this option to specify that the rule should be applied only during certain hours of the day. You must then use the fields and drop-down lists provided, to specify the desired time range.

Reordering Web Rules

500 1000N

To reorder Web rules

1. Click Security in the main menu, and click the Web Rules tab.

   The Web Rules page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Viewing and Deleting Web Rules

500 1000N

To view or delete an existing Web rule

1. Click Security in the main menu, and click the Web Rules tab.

   The Web Rules page appears with a list of existing Web rules.
2. To resize a column, drag the relevant column divider right or left.
3. To delete a rule, do the following.

   a. In the desired rule's row, click .
   A confirmation message appears.
   b. Click OK.
   The rule is deleted.

Enabling/Disabling Web Rule Logging

500 1000N

You can enable or disable logging for a Web rule, by using the information in ***Adding and Editing Web Rules*** on page 568, or by using the following shortcut.

To enable/disable logging for a Web rule

1. Click Security in the main menu, and click the Web Rules tab.

   The Web Rules page appears.
2. Next to the desired rule, in the Log column, do one of the following:

   - To enable logging, click .

     The button changes to and logging is enabled for the rule.
   - To disable logging, click .

     The button changes to and logging is disabled for the rule.

Using Web Filtering

500 1000N

When the Web Filtering service is enabled, access to Web content is restricted according to the categories specified in the Allow Categories area of the Web Filtering page.

Note: The Web Filtering service is only available if you are connected to a Service Center and subscribed to this service. For information on using subscription services, see ***Using Subscription Services*** on page *591*.

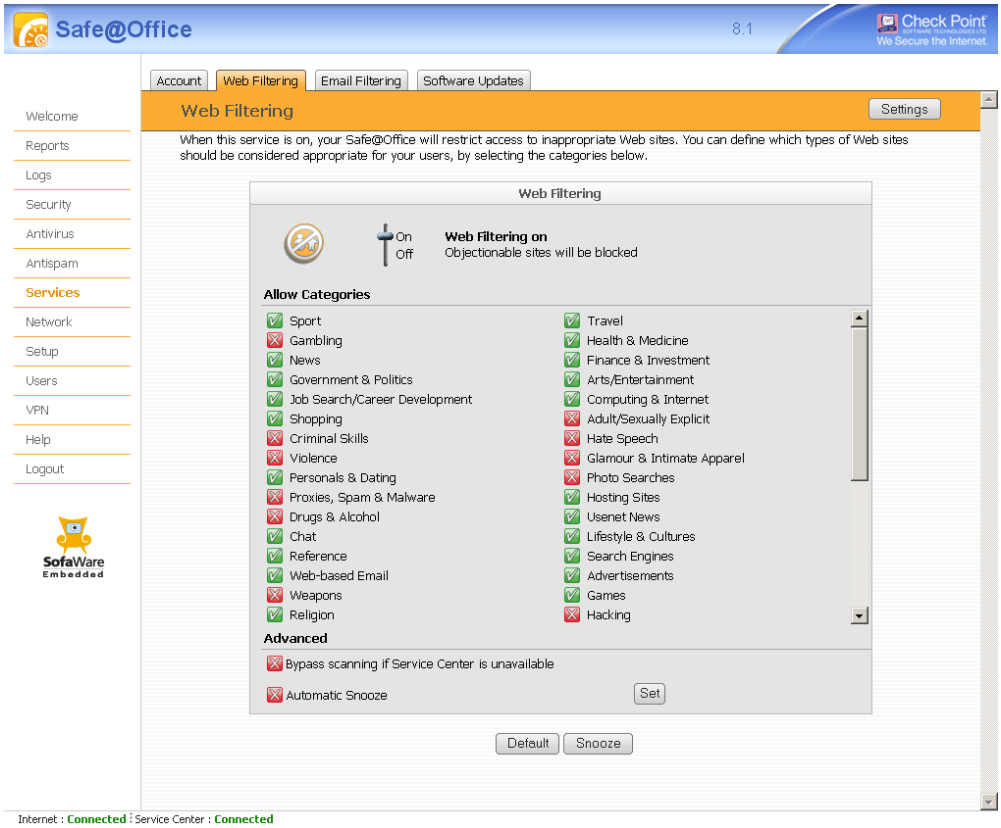
Enabling/Disabling Web Filtering

500 1000N

To enable/disable Web Filtering

1. Click Services in the main menu, and click the Web Filtering tab.

The Web Filtering page appears.



2. Drag the On/Off lever upwards or downwards.

   Web Filtering is enabled/disabled.

Selecting Categories for Blocking

500 1000N

You can define which types of Web sites should be considered appropriate for your family or office members, by selecting the categories. Categories marked with ✅ will remain visible, while categories marked with ❌ will be blocked and will require the administrator password for viewing.

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

Note: The list of supported categories may vary, depending on the Service Center to which the Safe@Office appliance is connected.

To allow/block a category

1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

2. In the Allow Categories area, use the scroll bar to scroll through all of the categories.

3. Click ✅ or ❌ next to the desired category.

Configuring Web Filtering Advanced Settings

500 1000N

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To configure Web Filtering advanced settings

1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

2. Next to the Bypass scanning if Service Center is unavailable option, specify how the gateway should handle Web Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all connections to the Internet, click .

     This ensures that users will not gain access to undesirable Web sites, even when the Service Center is unavailable.

     The button changes to .

   - To temporarily allow all connections to the Internet, click .

     This ensures continuous access to the Internet.

     The button changes to .

   When the Service Center is available again, the gateway will enforce the configured Web Filtering policy.

Temporarily Disabling Web Filtering

500 1000N

If desired, you can temporarily disable the Web Filtering service.

To temporarily disable Web Filtering

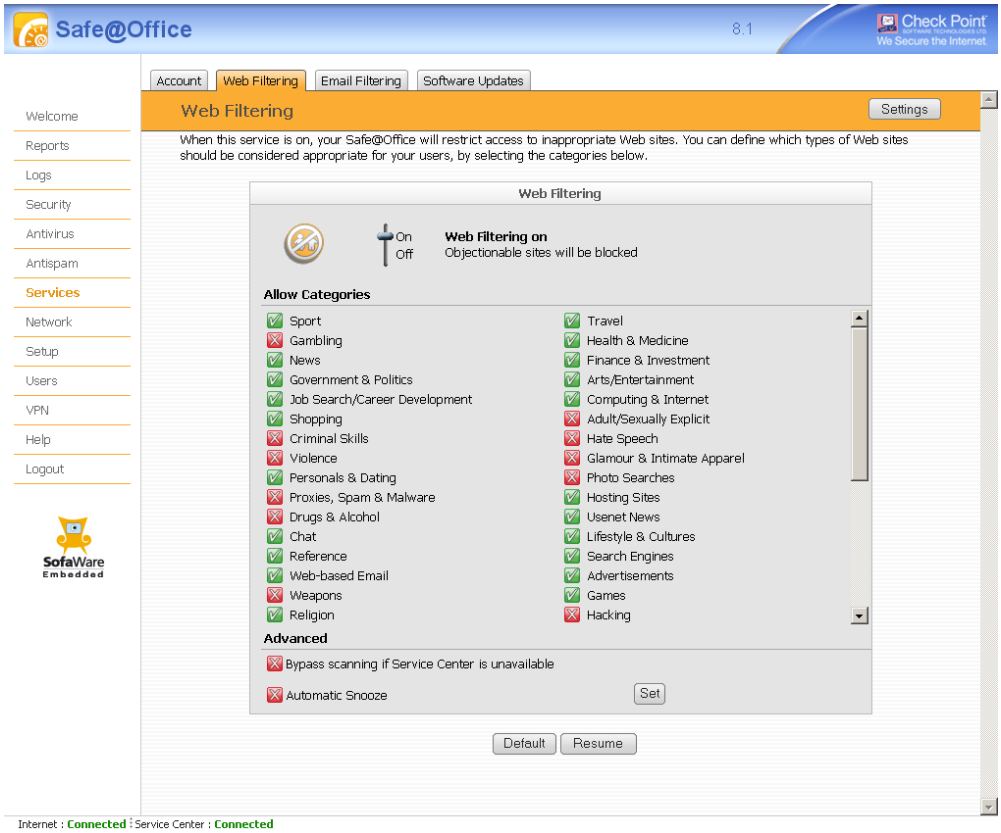
1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

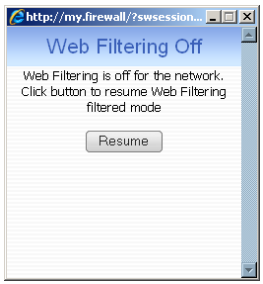
2. Click Snooze.

   - Web Filtering is temporarily disabled for all internal network computers.

- The Snooze button changes to Resume.



- The Web Filtering Off popup window opens.


http://my.firewall/?swsession...
Web Filtering Off
Web Filtering is off for the network. Click button to resume Web Filtering filtered mode
Resume

3. To re-enable the service, click Resume, either in the popup window, or on the Web Filtering page.

- The service is re-enabled for all internal network computers.
- If you clicked Resume in the Web Filtering page, the button changes to Snooze.
- If you clicked Resume in the Web Filtering Off popup window, the popup window closes.

Configuring Automatic Snooze

500 1000N

You can automatically disable the Web Filtering service during certain hours of the day, by configuring Automatic Snooze.

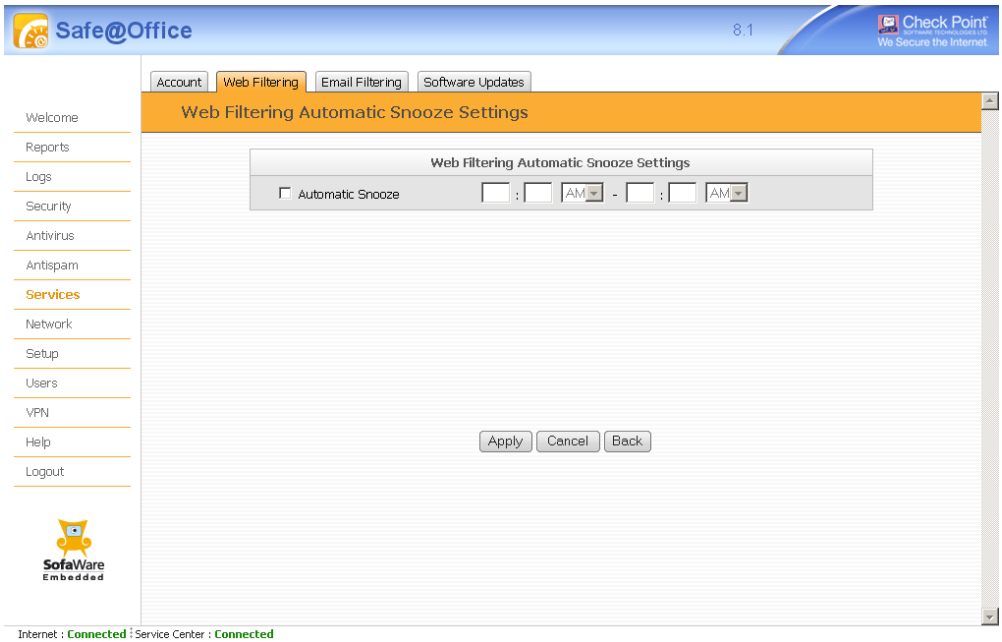
To configure Automatic Snooze

1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

2. In the Advanced area, next to Automatic Snooze, click Set.

The Web Filtering Automatic Snooze Settings page appears.



3. Do one of the following:

   - To enable Automatic Snooze:
     1) Select the Automatic Snooze check box.
     2) In the fields provided, specify the hours between which the Web Filtering service should be disabled.
   - To disable Automatic Snooze, clear the Automatic Snooze check box.

4. Click Apply.

   Automatic Snooze is enabled/disabled.

   If you enabled Automatic Snooze, the Web Filtering page displays the hours during which the Web Filtering service will be disabled.

Resetting Web Filtering Categories to Defaults

500 1000N

If desired, you can reset the Web Filtering categories to their default settings.

To restore Web Filtering defaults

1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

2. Click Defaults

   A confirmation message appears.

3. Click OK.

Customizing the Access Denied Page

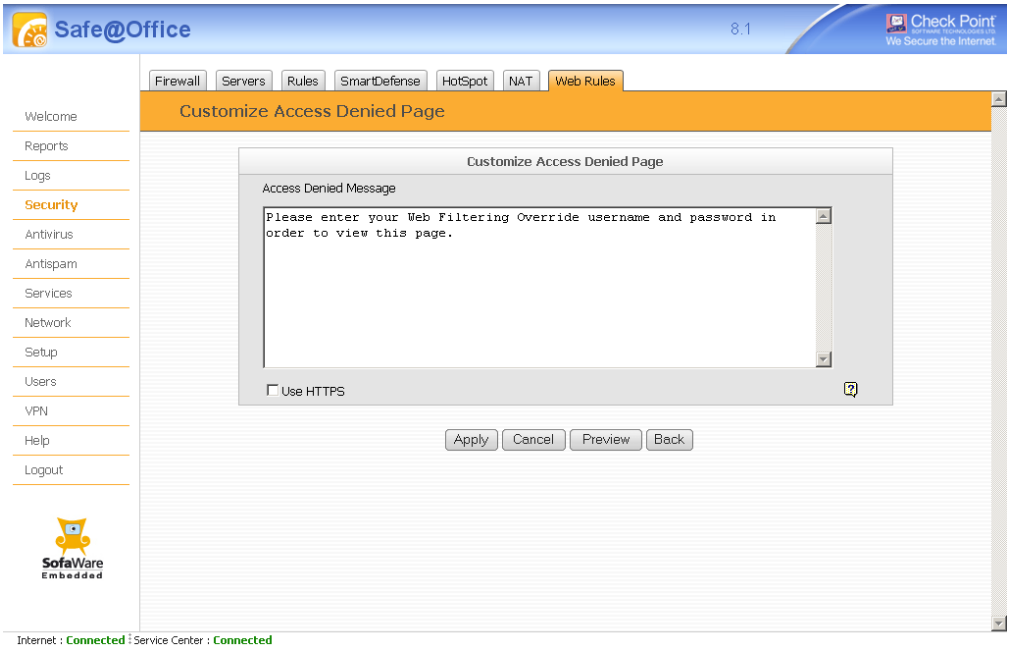
Power Pack

The Access Denied page appears when a user attempts to access a page that is blocked either by a Web rule or by the Web Filtering service. You can customize this page using the following procedure.

To customize the Access Denied page

1. Do one of the following:
   - Click Security in the main menu, and click the Web Rules tab.
     The Web Rules page appears.
   - Click Services in the main menu, and click the Web Filtering tab.
     The Web Filtering page appears.
2. Click Settings.

The Customize Access Denied Page page appears. In the following example, this page was accessed via the Web Rules page.



3. In the text box, type the message that should appear when a user attempts to access a blocked Web page.

   You can use HTML tags as needed.

4. To display the Access Denied page using HTTPS, select the Use HTTPS check box.

5. To preview the Access Denied page, click Preview.

   A browser window opens displaying the Access Denied page.

6. Click Apply.

   Your changes are saved.

Chapter 17

Updating the Firmware

This chapter explains how to update the Safe@Office appliance's firmware.

This chapter includes the following topics:

Overview 585
Using Software Updates 586
Updating the Firmware Manually.....588

Overview

You can update your Safe@Office appliance with new product features and protection against new security threats. To do so, you must update your appliance's firmware, by using one of the following methods:

- Software Updates. This subscription service allows checking for new security and software updates, either automatically or manually. Detected updates are downloaded and installed without user intervention.
- Manual updates. If you are not subscribed to the Software Updates service, you must update the firmware manually.

Note: To obtain firmware updates, whether via the Software Updates service, or for the purpose of updating you appliance manually, you must purchase a support/software subscription plan for your appliance.

Using Software Updates

500 1000N

Checking for Software Updates when Remotely Managed

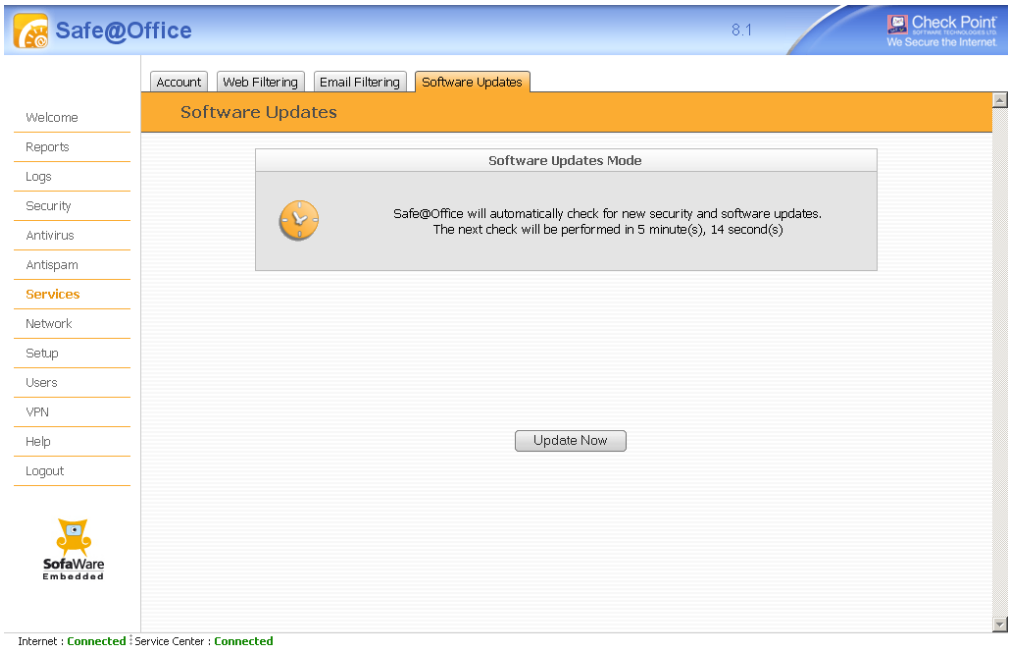
500 1000N

If your Safe@Office appliance is remotely managed, it automatically checks for software updates and installs them without user intervention. However, you can still check for updates manually, if needed.

To manually check for security and software updates

1. Click Services in the main menu, and click the Software Updates tab.

   The Software Updates page appears.



2. Click Update Now.

The system checks for new updates and installs them.

Checking for Software Updates when Locally Managed

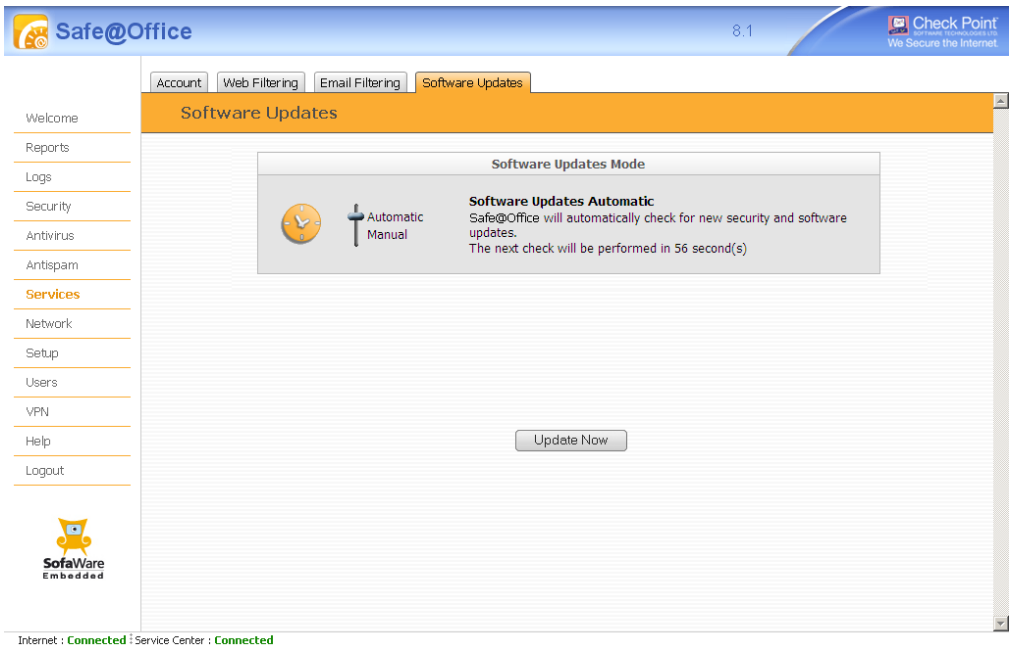
500 1000N

If your Safe@Office appliance is locally managed, you can set it to automatically check for software updates, or you can set it so that software updates must be checked for manually.

To configure software updates when locally managed

1. Click Services in the main menu, and click the Software Updates tab.

   The Software Updates page appears.



2. To set the Safe@Office appliance to automatically check for and install new software updates, drag the Automatic/Manual lever upwards.

   The Safe@Office appliance checks for new updates and installs them according to its schedule.

Note: When the Software Updates service is set to Automatic, you can still manually check for updates.

3. To set the Safe@Office appliance so that software updates must be checked for manually, drag the Automatic/Manual lever downwards.

   The Safe@Office appliance does not check for software updates automatically.

4. To manually check for software updates, click Update Now.

   The system checks for new updates and installs them.

Updating the Firmware Manually

500 | 1000N

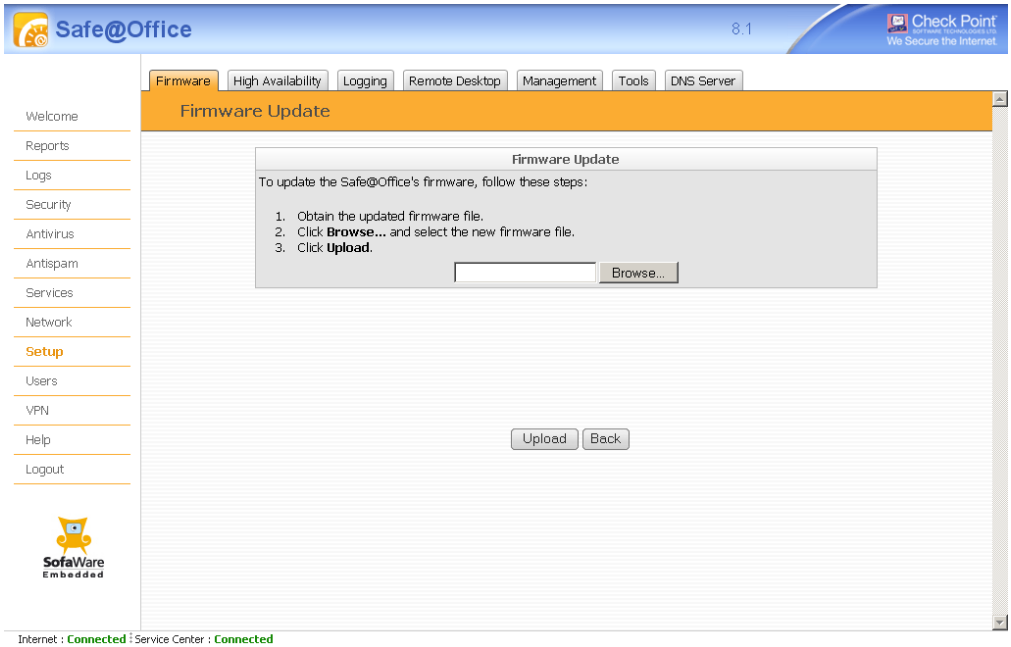
Updating the Safe@Office firmware manually

1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.

2. Click Firmware Update.

The Firmware Update page appears.



3. Click Browse.

   A browse window appears.

4. Select the image file and click Open.

   The Firmware Update page reappears. The path to the firmware update image file appears in the Browse text box.

5. Click Upload.

   Your Safe@Office appliance firmware is updated.

   Updating may take a few minutes. Do not power off the appliance.

   At the end of the process the Safe@Office appliance restarts automatically.

Chapter 18

Using Subscription Services

This chapter explains how to connect your Safe@Office appliance to a Service Center and start subscription services.

Note: Check with your reseller regarding availability of subscription services, or surf to www.sofaware.com/servicecenters to locate a Service Center in your area.

This chapter includes the following topics:

Connecting to a Service Center 591
Viewing Services Information 597
Refreshing Your Service Center Connection 598
Configuring Your Account 599
Disconnecting from Your Service Center 599

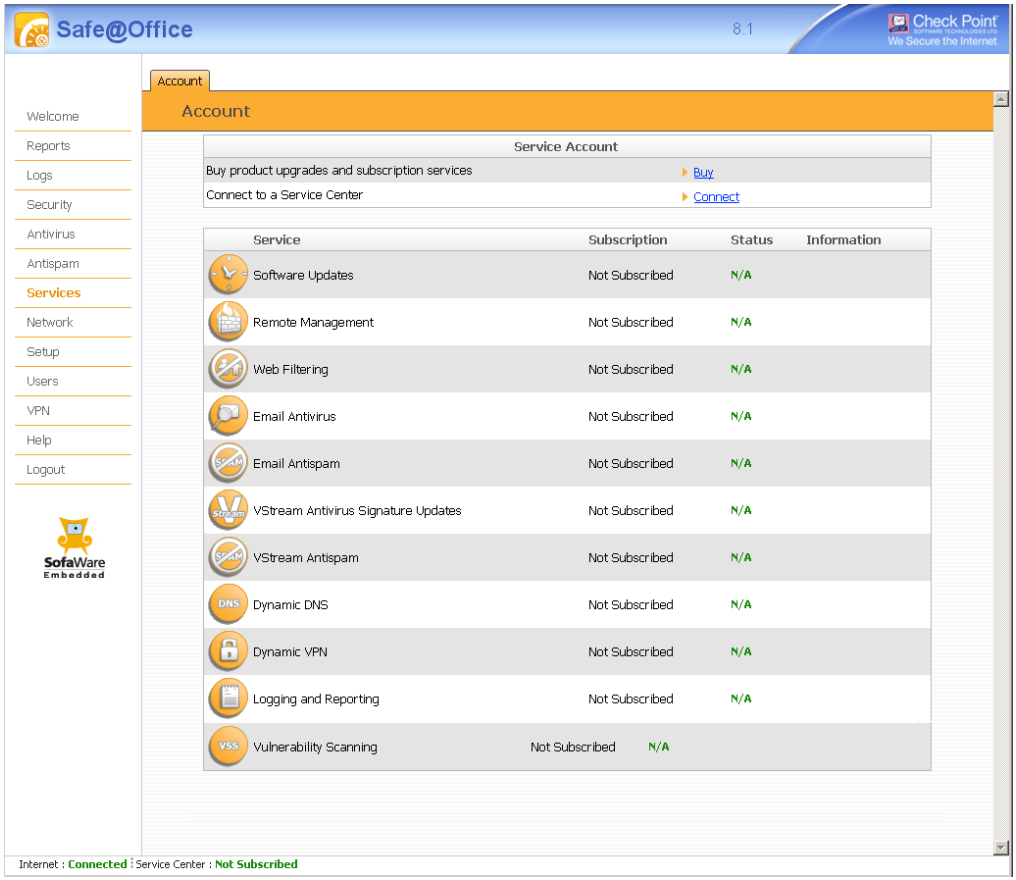
Connecting to a Service Center

500 1000N

To connect to a Service Center

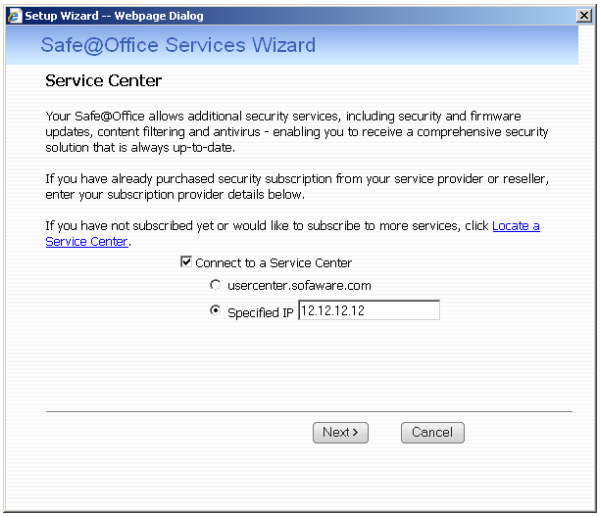
1. Click Services in the main menu, and click the Account tab.

The Account page appears.



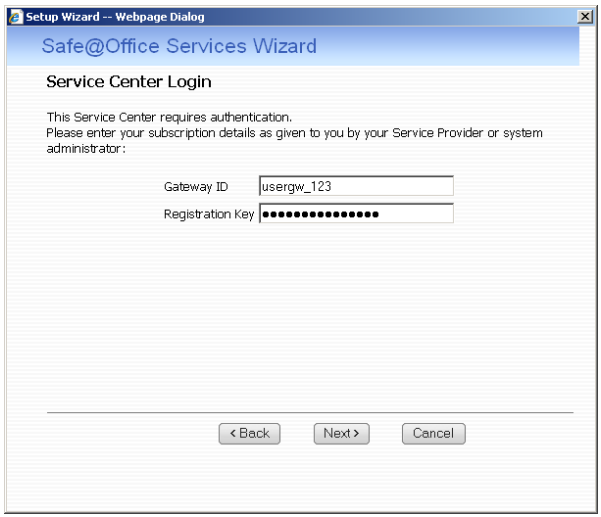
2. In the Service Account area, click Connect.

The Safe@Office Services Wizard opens, with the Service Center dialog box displayed.


Setup Wizard -- Webpage Dialog
Safe@Office Services Wizard
Service Center
Your Safe@Office allows additional security services, including security and firmware updates, content filtering and antivirus - enabling you to receive a comprehensive security solution that is always up-to-date.
If you have already purchased security subscription from your service provider or reseller, enter your subscription provider details below.
If you have not subscribed yet or would like to subscribe to more services, click Locate a Service Center.
Connect to a Service Center
usercenter.sofaware.com
Specified IP
12.12.12.12
Next >
Cancel

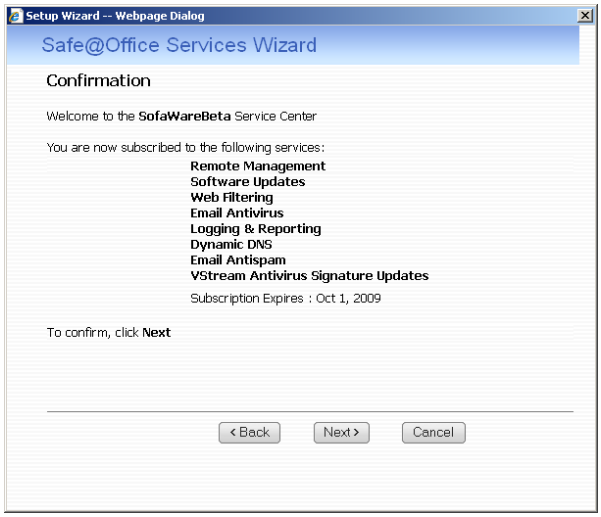
3. Make sure the Connect to a Service Center check box is selected.
4. Do one of the following:
   - To connect to the SofaWare Service Center, choose usercenter.sofaware.com.
   - To specify a Service Center, choose Specified IP and then in the Specified IP field, enter the desired Service Center's IP address, as given to you by your system administrator.
5. Click Next.
   - The Connecting screen appears.

- If the Service Center requires authentication, the Service Center Login dialog box appears.


Setup Wizard -- Webpage Dialog
Safe@Office Services Wizard
Service Center Login
This Service Center requires authentication.
Please enter your subscription details as given to you by your Service Provider or system administrator:
Gateway ID
usergw_123
Registration Key
< Back
Next >
Cancel

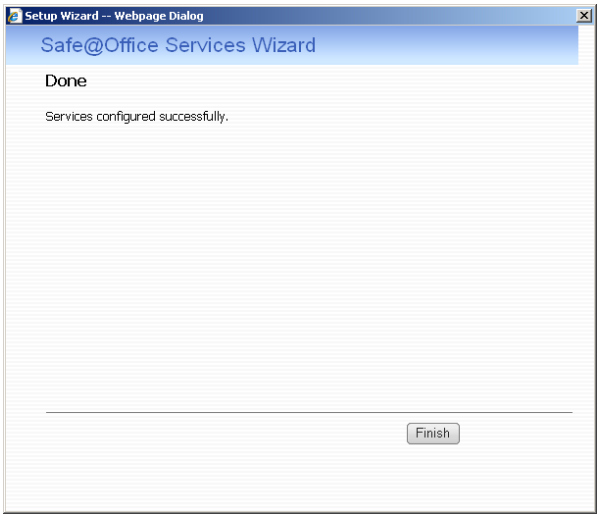
Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider, then click Next.

- The Connecting screen appears.
- The Confirmation dialog box appears with a list of services to which you are subscribed.



6. Click Next.

   The Done screen appears with a success message.

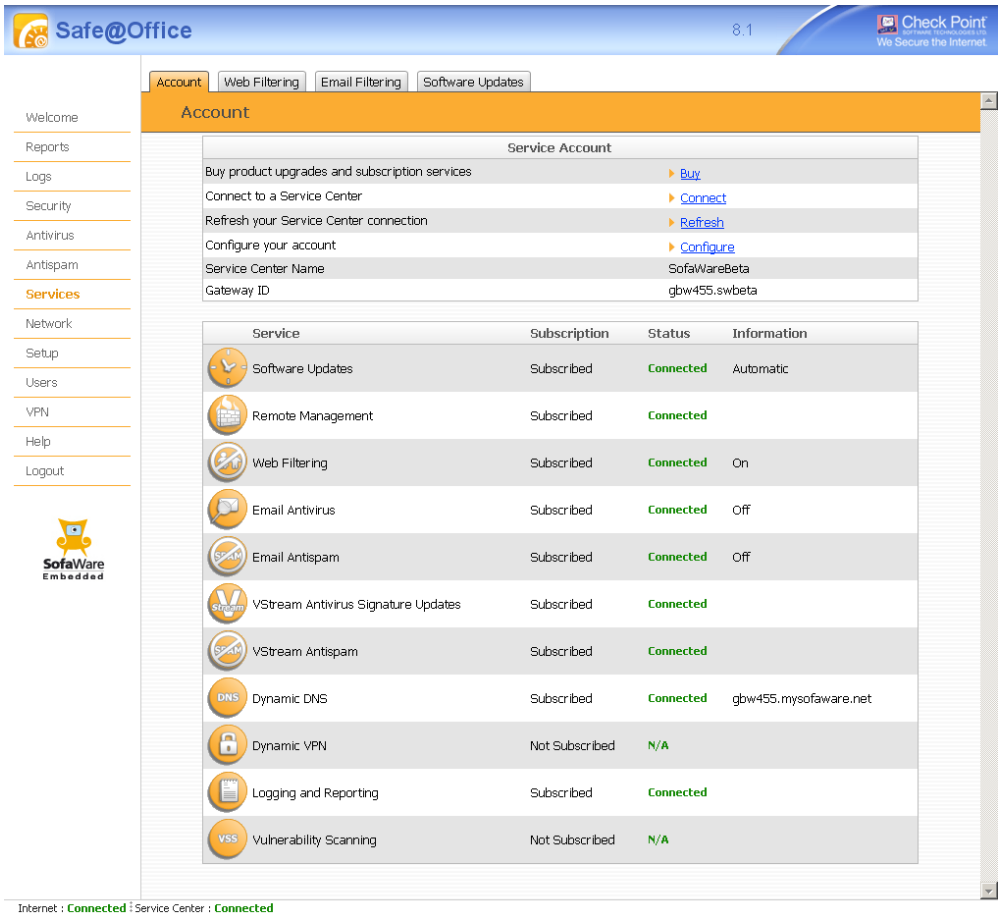


7. Click Finish.

   The following things happen:

   - If a new firmware is available, the Safe@Office appliance may start downloading it. This may take several minutes. Once the download is complete, the Safe@Office appliance restarts using the new firmware.
   - The Welcome page appears.

- The services to which you are subscribed are now available on your Safe@Office appliance and listed as such on the Account page. See ***Viewing Services Information*** on page 597 for further information.



- The Services submenu includes the services to which you are subscribed.

Viewing Services Information

500 1000N

The Account page displays the following information about your subscription.

Table 129: Account Page Fields

This field…	Displays…
Service Center Name	The name of the Service Center to which you are connected (if known).
Gateway ID	Your gateway ID.
Subscription will end on	The date on which your subscription to services will end.
Service	The services available in your service plan.
Subscription	The status of your subscription to each service: • Subscribed • Not Subscribed
Status	The status of each service: • Connected. You are connected to the service through the Service Center. • Connecting. Connecting to the Service Center. • N/A. The service is not available.
Information	The mode to which each service is set. If you are subscribed to Dynamic DNS, this field displays your gateway's domain name. For further information, see ***Web Filtering*** on page 575, ***Virus Scanning*** on page 558, and ***Automatic and Manual Updates*** on page 586.

Refreshing Your Service Center Connection

500 1000N

This option restarts your Safe@Office appliance's connection to the Service Center and refreshes your Safe@Office appliance's service settings.

To refresh your Service Center connection

1. Click Services in the main menu, and click the Account tab.

   The Account page appears.

2. In the Service Account area, click Refresh.

   The Safe@Office appliance reconnects to the Service Center.

   Your service settings are refreshed.

Configuring Your Account

500

This option allows you to access your Service Center's Web site, which may offer additional configuration options for your account. Contact your Service Center for a user ID and password.

To configure your account

1. Click Services in the main menu, and click the Account tab.

   The Account page appears.

2. In the Service Account area, click Configure.

Note: If no additional settings are available from your Service Center, this button will not appear.

   Your Service Center's Web site opens.

3. Follow the on-screen instructions.

Disconnecting from Your Service Center

500 1000N

If desired, you can disconnect from your Service Center.

To disconnect from your Service Center

1. Click Services in the main menu, and click the Account tab.

   The Account page appears.

2. In the Service Account area, click Connect.

   The Safe@Office Services Wizard opens, with the first Subscription Services dialog box displayed.

3. Clear the Connect to a Service Center check box.

4. Click Next.

   The Done screen appears with a success message.

5. Click Finish.

   The following things happen:

   - You are disconnected from the Service Center.
   - The services to which you were subscribed are no longer available on your Safe@Office appliance.

Chapter 19

Working With VPNs

This chapter describes how to use your Safe@Office appliance as a Remote Access VPN Client, server, or gateway.

This chapter includes the following topics:

Overview 601
Setting Up Your Safe@Office Appliance as a VPN Server 607
Adding and Editing VPN Sites 621
Viewing and Deleting VPN Sites 654
Enabling/Disabling a VPN Site 654
Logging in to a Remote Access VPN Site 655
Logging Out of a Remote Access VPN Site 658
Using Certificates 658
Viewing VPN Tunnels 670
Viewing IKE Traces for VPN Connections 673
Viewing VPN Topology 674

Overview

You can configure your Safe@Office appliance as part of a virtual private network (VPN). A VPN is a private data network consisting of a group of gateways that can securely connect to each other. Each member of the VPN is called a *VPN site*, and a connection between two VPN sites is called a *VPN tunnel*. VPN tunnels encrypt and authenticate all traffic passing through them. Through these tunnels, employees can safely use their company's network resources when working at home. For example, they can securely read email, use the company's intranet, or access the company's database from home.

The Safe@Office appliance supports the following types of VPN sites:

- SecuRemote Remote Access VPN Server. Makes a network remotely available to authorized users who connect to the Remote Access VPN Server using the Check Point SecuRemote VPN Client (provided for free with your Safe@Office) or another Safe@Office.

- SecuRemote Internal VPN Server. SecuRemote can also be used from your internal networks, allowing you to secure your wired or wireless network with strong encryption and authentication.
- Endpoint Connect VPN Server. Makes a network available to authorized users who connect from the Internet or from your internal networks using the Check Point Endpoint Connect VPN Client. Endpoint Connect provides mobile users with seamless connectivity to corporate resources, by encrypting and authenticating data transmitted during secure remote access sessions.
- L2TP VPN Server. Makes a network available to authorized users who connect from the Internet or from your internal networks using an L2TP client such as the Microsoft L2TP IPSec VPN Client.
- Site-to-Site VPN Gateway. Can connect with another Site-to-Site VPN Gateway in a permanent, bi-directional relationship.
- Remote Access VPN Client. Can connect to a Remote Access VPN Server, but other VPN sites cannot initiate a connection to the Remote Access VPN Client. Defining a Remote Access VPN Client is a hardware alternative to using remote access software.

All Safe@Office models provide full VPN functionality. They can act as a Remote Access VPN Client, a Remote Access VPN Server for multiple users, or a Site-to-Site VPN Gateway.

A virtual private network (VPN) must include at least one Remote Access VPN Server or gateway. The type of VPN sites you include in a VPN depends on the type of VPN you want to create, Site-to-Site or Remote Access.

Note: A locally managed Remote Access VPN Server or gateway must have a static IP address. If you need a Remote Access VPN Server or gateway with a dynamic IP address, you must use SofaWare Security Management Portal (SMP) management.

A SecuRemote/SecureClient/L2TP/Endpoint Connect or Safe@Office Remote Access VPN Client can have a dynamic IP address, regardless of whether it is locally or remotely managed.

Note: This chapter explains how to define a VPN locally. However, if your appliance is centrally managed by a Service Center, then the Service Center can automatically deploy VPN configuration for your appliance.

Site-to-Site VPNs

A Site-to-Site VPN consists of two or more Site-to-Site VPN Gateways that can communicate with each other in a bi-directional relationship. The connected networks function as a single network. You can use this type of VPN to mesh office branches into one corporate network.

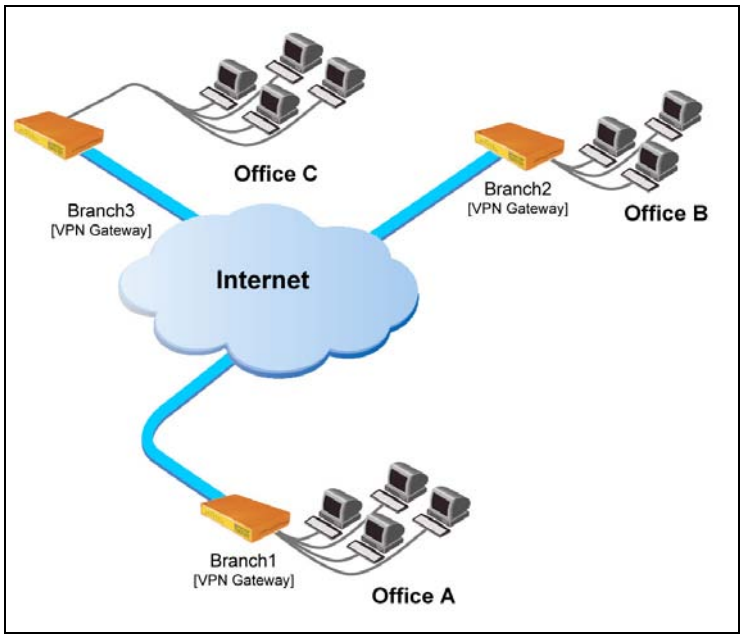


Figure 37: Site-to-Site VPN

To create a Site-to-Site VPN with two VPN sites

1. On the first VPN site's Safe@Office appliance, do the following:
   a. Define the second VPN site as a Site-to-Site VPN Gateway, using the procedure ***Adding and Editing VPN Sites*** on page 621.
   b. Enable a Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 607.
2. On the second VPN site's Safe@Office appliance, do the following:
   a. Define the first VPN site as a Site-to-Site VPN Gateway, using the procedure ***Adding and Editing VPN Sites*** on page 621.
   b. Enable a Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 607.

Note: You can manually configure each VPN site's internal encryption domain via the CLI. For information, refer to the *Embedded NGX CLI Reference Guide*.

Remote Access VPNs

A Remote Access VPN consists of one Remote Access VPN Server or Site-to-Site VPN Gateway, and one or more Remote Access VPN Clients. You can use this type of VPN to make an office network remotely available to authorized users, such as employees working from home, who connect to the office Remote Access VPN Server with their Remote Access VPN Clients.

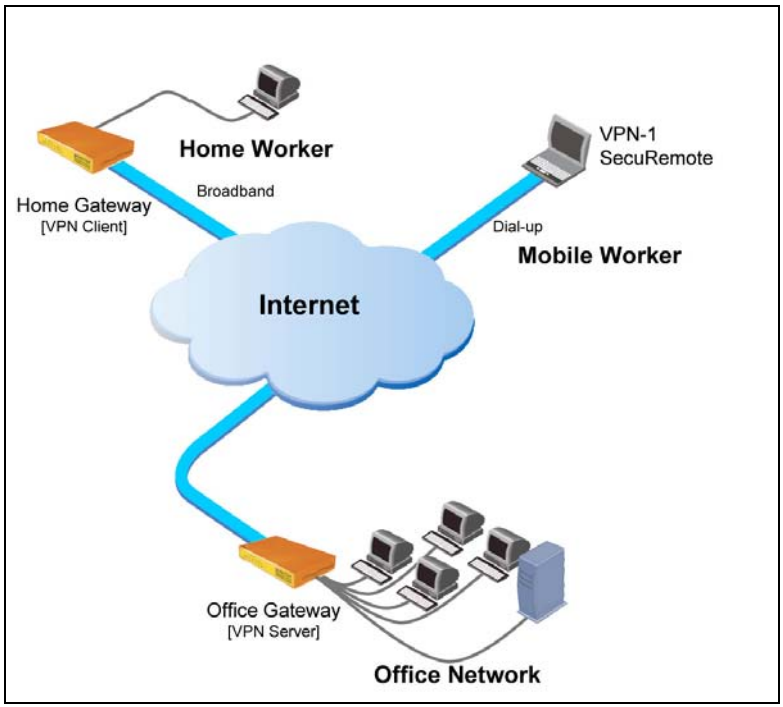


Figure 38: Remote Access VPN

To create a Remote Access VPN with two VPN sites

1. On the remote user VPN site's Safe@Office appliance, add the office Remote Access VPN Server as a Remote Access VPN site.

   See ***Adding and Editing VPN Sites*** on page 621.

   The remote user's Safe@Office appliance will act as a Remote Access VPN Client.

2. On the office VPN site's Safe@Office appliance, enable a Remote Access VPN Server.

   See ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 607.

Internal VPN Server

You can use your Safe@Office appliance as an internal VPN Server, for enhanced wired and wireless security. When an internal VPN Server is enabled, internal network PCs and PDAs with the appropriate software installed can establish a Remote Access VPN session to the gateway. This means that connections from internal network users to the gateway can be encrypted and authenticated.

The benefits of using an internal VPN Server are two-fold:

- Accessibility

  Using SecureClient, Endpoint Connect, or L2TP, you can enjoy a secure connection from anywhere—in your wireless network or on the road—without changing any settings. The standard is completely transparent and allows you to access company resources the same way, whether you are sitting at your desk or anywhere else.

  Note: Only SecureClient and Endpoint Connect can connect to the SecuRemote Internal VPN server, not SecuRemote.

- Security

  Many of today's attacks are increasingly introduced from inside the network. Internal security threats cause outages, downtime, and lost revenue. Wired networks that deal with highly sensitive information—especially networks in public places, such as classrooms—are vulnerable to users trying to hack the internal network.

  Using an internal VPN Server, along with a strict security policy for non-VPN users, can enhance security both for wired networks and for wireless networks, which are particularly vulnerable to security breaches.

For information on setting up your Safe@Office appliance as an internal VPN Server, see ***Configuring the Internal VPN Server*** on page 610.

Setting Up Your Safe@Office Appliance as a VPN Server

500 1000N

You can make your network available to authorized users connecting from the Internet or from your internal networks, by setting up your Safe@Office appliance as a VPN Server.

When the SecuRemote Remote Access VPN Server or SecuRemote Internal VPN Server is enabled, users can connect to the server via Check Point SecuRemote/SecureClient or via a Safe@Office appliance in Remote Access VPN mode.

The Endpoint Connect VPN Server can be enabled *in addition* to one or more of the SecuRemote VPN Servers, to allow users to connect from relevant locations using an Endpoint Connect VPN Client. For example, if both the SecuRemote Remote Access VPN Server and the Endpoint Connect VPN Server are enabled, but the SecuRemote Internal VPN Server is *not* enabled, then users will be able to use the Endpoint Connect VPN Client to connect from the Internet but not from your internal networks. Endpoint Connect users are automatically assigned to the OfficeMode network, enabling you to configure special security rules for them.

When the L2TP (Layer 2 Tunneling Protocol) VPN Server is enabled, users can connect to the server using an L2TP client such as the Microsoft Windows L2TP IPSEC VPN Client. L2TP users are automatically assigned to the OfficeMode network, enabling you to configure special security rules for them.

SecuRemote/SecureClient supports split tunneling, which means that VPN Clients can connect directly to the Internet, while traffic to and from VPN sites passes through the VPN Server. In contrast, the L2TP VPN Client does not support split tunneling, meaning that all Internet traffic to and from a VPN Client passes through the VPN Server and is routed to the Internet.

Enabling the Safe@Office VPN Server for users connecting from your internal networks adds a layer of security to such connections. For example, while you could create a firewall rule allowing a specific user on the DMZ to access the LAN, enabling VPN access for the user means that such connections can be encrypted and authenticated. For more information, see ***Internal VPN Server*** on page 606.

Note: The use of all Remote VPN Clients is subject to Check Point's purchasing terms and conditions.

To set up your Safe@Office appliance as a VPN Server

1. Configure the VPN Server in one or more of the following ways:
   - To accept SecuRemote/SecureClient or Safe@Office remote access connections from the Internet.

     See ***Configuring the SecuRemote Remote Access VPN Server*** on page 609.
   - To accept SecuRemote/SecureClient connections from your internal networks.

     See ***Configuring the SecuRemote Internal VPN Server*** on page 610.
   - To accept Endpoint Connect remote access connections from the Internet and/or from your internal networks.

     See ***Configuring the Endpoint Connect VPN Server*** on page 611.
   - To accept L2TP remote access connections from the Internet, as well L2TP connections from your internal networks.

     See ***Configuring the L2TP VPN Server*** on page 612.
2. If you configured the SecuRemote Internal VPN Server, install SecuRemote/SecureClient on the desired internal network computers.

   See ***Installing SecuRemote*** on page 613.
3. If you configured both the SecuRemote Internal VPN Server *and* the Endpoint Connect VPN Server, install Endpoint Connect on the desired internal network computers.

   See ***Installing Endpoint Connect*** on page 613.
4. If you configured the L2TP VPN Server, do the following:
   a. Configure the OfficeMode network.

      See ***Configuring the OfficeMode Network*** on page 214.

      All users connecting via L2TP will be assigned to the OfficeMode network.
   b. Configure L2TP VPN Clients on the desired internal network computers.

      See ***Configuring L2TP VPN Clients*** on page 614.
5. Set up remote VPN access for users.

See ***Setting Up Remote VPN Access for Users*** on page 687.

Note: Disabling the VPN Server for a specific type of connection will cause all existing VPN tunnels of that type to disconnect.

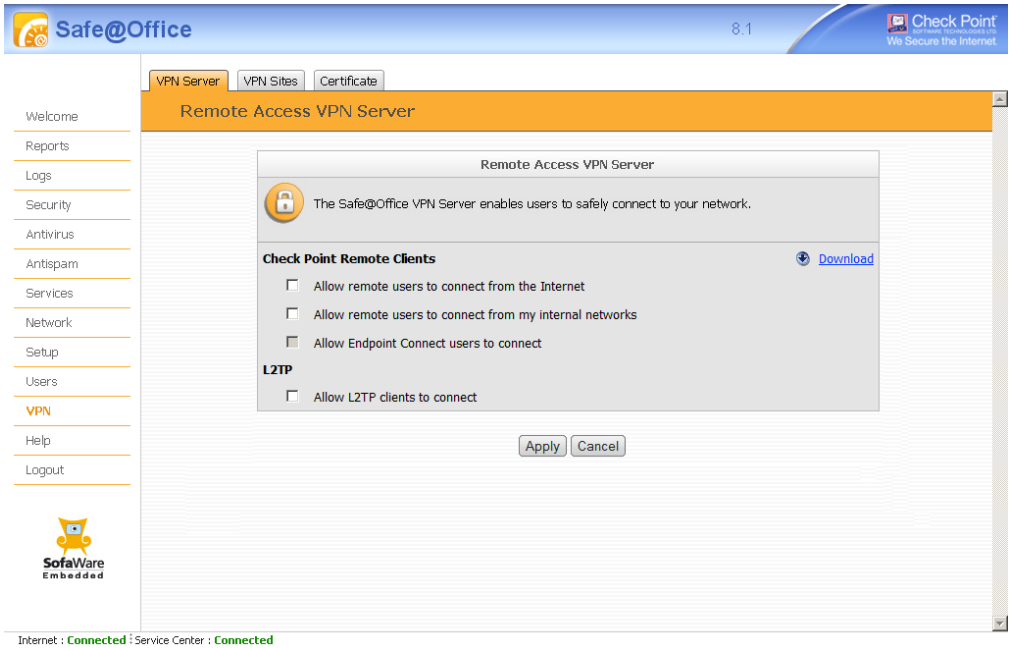
Configuring the SecuRemote Remote Access VPN Server

500 1000N

To configure the SecuRemote Remote Access VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.



2. Select the Allow remote users to connect from the Internet check box.

   New check boxes appear.

3. To allow authenticated users connecting from the Internet to bypass NAT when connecting to your internal network, select the Bypass NAT check box.

4. To allow authenticated users connecting from the Internet to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

5. Click Apply.

   The SecuRemote Remote Access VPN Server is enabled for the specified connection types.

Configuring the SecuRemote Internal VPN Server

500 1000N

To configure the SecuRemote Internal VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Select the Allow remote users to connect from my internal networks check box.

   New check boxes appear.

3. To allow authenticated users connecting from internal networks to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

Note: Bypass NAT is always enabled for the SecuRemote Internal VPN Server, and cannot be disabled.

4. Click Apply.

   The SecuRemote Internal VPN Server is enabled for the specified connection types.

Configuring the Endpoint Connect VPN Server

500 1000N

To configure the Endpoint Connect VPN Server

1. Do one or more of the following:
   - To accept Endpoint Connect remote access connections from the Internet, configure the SecuRemote Remote Access VPN Server.

     See ***Configuring the SecuRemote Remote Access VPN Server*** on page 609.
   - To accept Endpoint Connect connections from your internal networks, configure the SecuRemote Internal VPN Server.

     See ***Configuring the SecuRemote Internal VPN Server*** on page 610.
2. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.
3. Select the Allow Endpoint Connect users to connect check box.

   The Listening Port field appears.
4. (Optional) In the Listening Port field, type the TCP port on which the appliance should accept incoming Endpoint Connect connection requests.

   The default listening port is 443.
5. Click Apply.

   The Endpoint Connect Remote Access VPN Server is enabled.

Configuring the L2TP VPN Server

500 1000N

To configure the L2TP VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Select the Allow L2TP clients to connect check box.

   New check boxes appear.

3. In the Preshared Secret field, type the preshared secret to use for secure communications between the L2TP clients and the VPN Server.

   The secret can contain spaces and special characters. It is used to secure L2TP connections for all users.

   In addition to entering this secret, each L2TP user will have to authenticate with a username and password.

   For information on defining users with VPN access permissions, see ***Setting Up Remote VPN Access for Users*** on page 687.

4. To allow authenticated users to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

5. Click Apply.

   The L2TP VPN Server is enabled for the specified connection types.

Installing SecuRemote

500 1000N

If you configured the SecuRemote Internal VPN Server, you must install the SecuRemote/SecureClient VPN Client on all internal network computers that should be allowed to remotely access your network via SecuRemote connections.

To install SecureClient/SecuRemote

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Click the Download link.

   The VPN clients for UTM-1 Edge and Safe@Office page opens in a new window.

3. Follow the online instructions to complete installation.

   SecureClient/SecuRemote is installed.

   For information on using SecureClient/SecuRemote, see the User Help. To access SecureClient/SecuRemote User Help, right-click on the VPN Client icon in the taskbar, select Settings, and then click Help.

Installing Endpoint Connect

500 1000N

If you configured the Endpoint Connect Internal VPN Server, you must install the Endpoint Connect VPN Client on all computers that should be allowed to remotely access your network.

To install Endpoint Connect

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Click the Download link.

   The VPN clients for UTM-1 Edge and Safe@Office page opens in a new window.

3. Follow the online instructions to complete installation.

   Endpoint Connect is installed.

Configuring L2TP VPN Clients

500 1000N

If you configured the L2TP VPN Server, you must configure the L2TP VPN Client on all computers that should be allowed to remotely access your network via L2TP connections.

This procedure is relevant for computers with a Windows XP operating system.

Note: The Safe@Office appliance supports the following authentication methods:

- PAP. For both local users and RADIUS users
- EAP-MD5, CHAP. For local users, but not for RADIUS users

To configure L2TP VPN Clients on Microsoft Windows

1. Click Start > Settings > Control Panel.

   The Control Panel window appears.

2. Double-click the Network and Dial-up Connections icon.

   The Network and Dial-up Connections window appears.

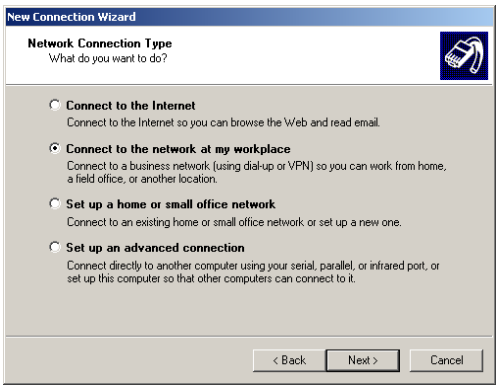
3. Click File > New Connection.

The New Connection Wizard opens displaying the Welcome to the New Connection Wizard screen.

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
• Connect to the Internet.
• Connect to a private network, such as your workplace network.
• Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

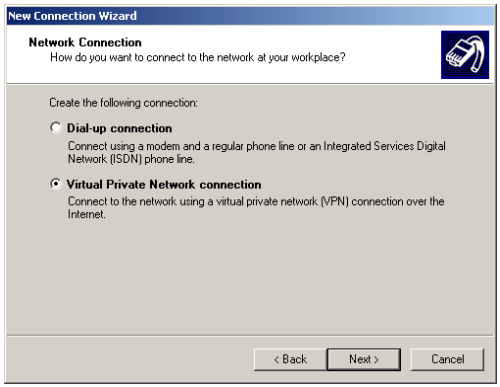
4. Click Next.

   The Network Connection Type dialog box appears.


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

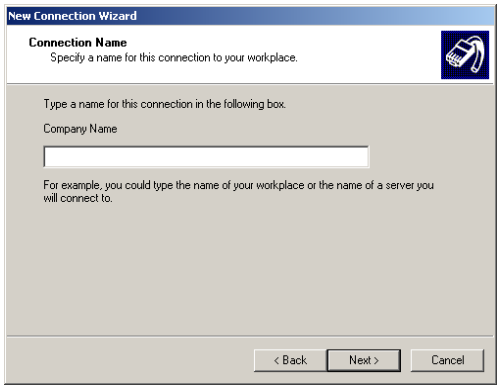
5. Choose Connect to the network at my workplace.
6. Click Next.

7. The Network Connection dialog box appears.


New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

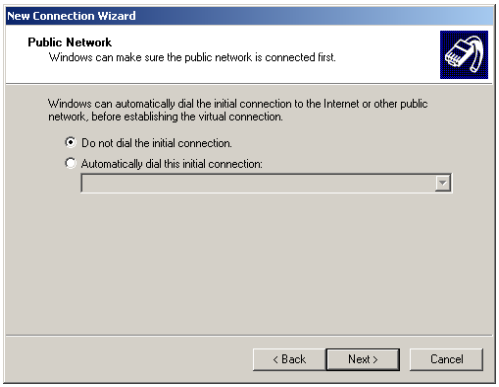
8. Choose Virtual Private Network connection.
9. Click Next.

   The Connection Name dialog box appears.


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

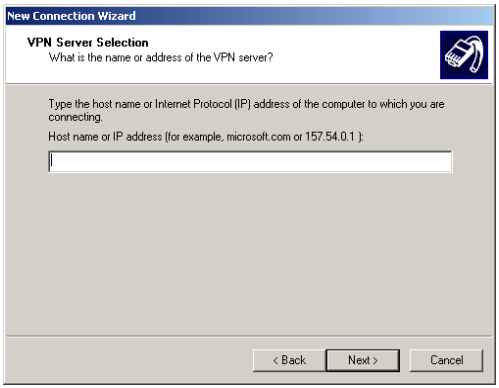
10. In the Company Name field, type your company's name.
11. Click Next.

The Public Network dialog box appears.


New Connection Wizard
Public Network
Windows can make sure the public network is connected first.
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.
Do not dial the initial connection.
Automatically dial this initial connection:
< Back
Next >
Cancel

12. Choose Do not dial the initial connection.
13. Click Next.

    The VPN Server Selection dialog box appears.


New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
< Back
Next >
Cancel

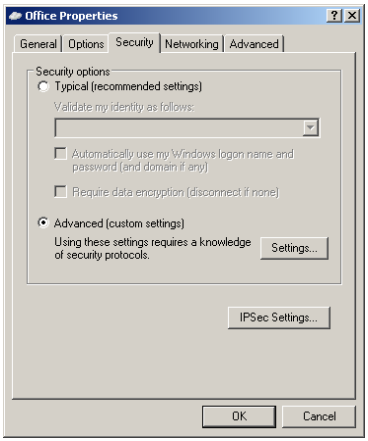
14. In the field, type the Safe@Office appliance's IP address.

The Completing the New Connection Wizard screen appears.

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
Office
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

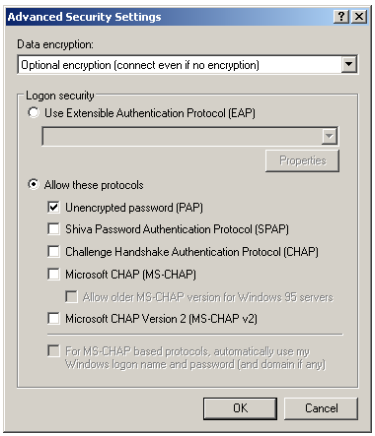
15. Click Finish.
16. In the Network and Dial-up Connections window, right-click on the L2TP connection, and click Properties in the popup menu.

    The connection's Properties dialog box opens.
17. In the Security tab, choose Advanced (custom settings).



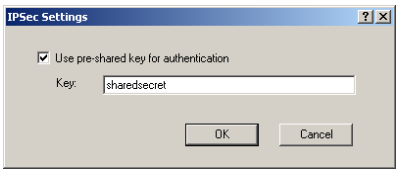
18. Click Settings.

The Advanced Security Settings dialog box opens.


Advanced Security Settings
Data encryption:
Optional encryption (connect even if no encryption)
Logon security
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Shiva Password Authentication Protocol (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Allow older MS-CHAP version for Windows 95 servers
Microsoft CHAP Version 2 (MS-CHAP v2)
For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)
OK
Cancel

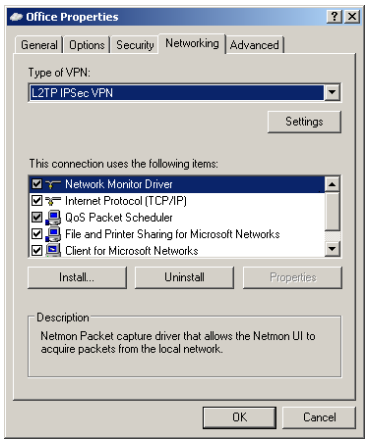
19. In the Data encryption drop-down list, select Optional encryption.
20. Choose Allow these protocols.
21. Select the Unencrypted password (PAP) check box, and clear all other check boxes.
22. Click OK.
23. In Properties dialog box's Security tab, click IPSec Settings.

    The IPSec Settings dialog box opens.



24. Select the Use pre-shared key for authentication check box.
25. In the Key field, type the preshared secret you configured on the L2TP VPN Server.
26. Click OK.
27. In Properties dialog box, click the Networking tab.

28. In the Type of VPN drop-down list, select L2TP IPSec VPN.



29. Click OK.

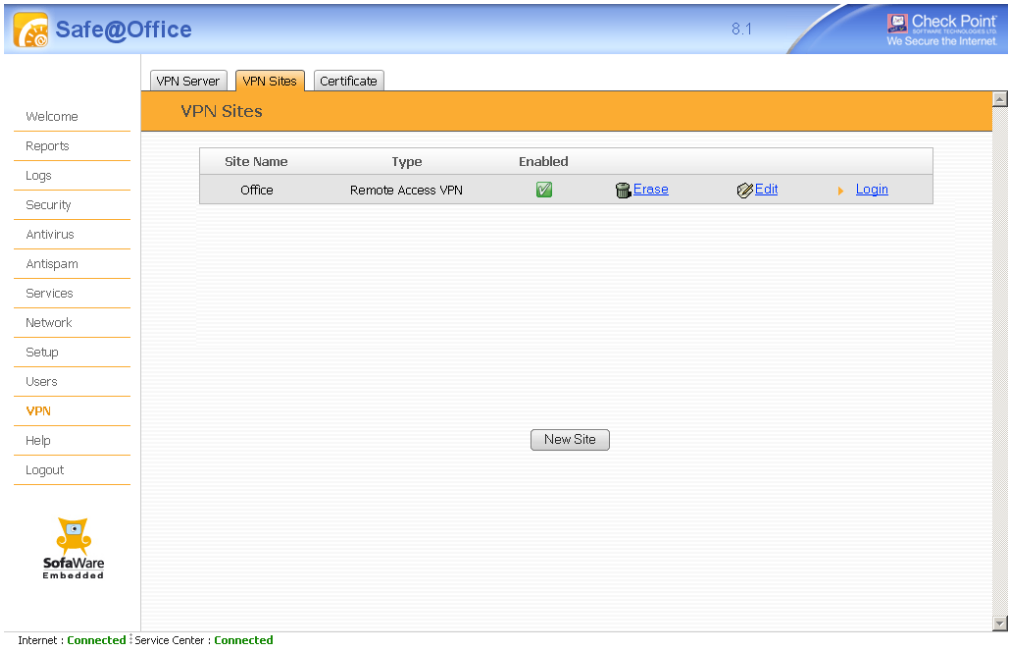
Adding and Editing VPN Sites

500 1000N

To add or edit VPN sites

1. Click VPN in the main menu, and click the VPN Sites tab.

   The VPN Sites page appears with a list of VPN sites.



2. Do one of the following:

   - To add a VPN site, click New Site.
   - To edit a VPN site, click Edit in the desired VPN site's row.

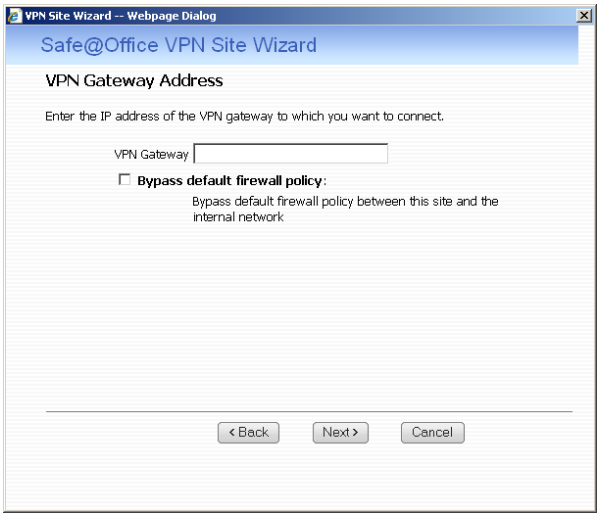
The Safe@Office VPN Site Wizard opens, with the Welcome to the VPN Site Wizard dialog box displayed.

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Welcome to the VPN Site Wizard
Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site.
Select the type of site to establish:
Remote Access VPN:
Allow a user to establish remote access sessions to another network.
Site-to-Site VPN:
Establishes a permanent secure link between your network and a remote network.
To continue, click Next.
Next >
Cancel

3. Do one of the following:
   - Select Remote Access VPN to establish remote access from your Remote Access VPN Client to a Remote Access VPN Server.
   - Select Site-to-Site VPN to create a permanent bi-directional connection to another Site-to-Site VPN Gateway.
4. Click Next.

Configuring a Remote Access VPN Site

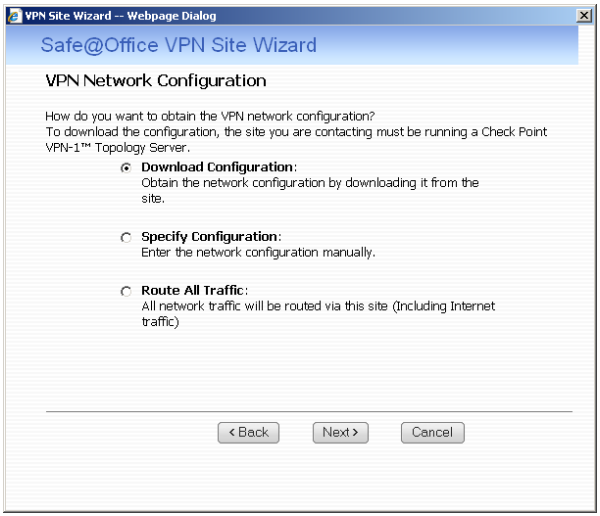
If you selected Remote Access VPN, the VPN Gateway Address dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Gateway Address
Enter the IP address of the VPN gateway to which you want to connect.
VPN Gateway
Bypass default firewall policy:
Bypass default firewall policy between this site and the internal network
< Back
Next >
Cancel

1. Enter the IP address of the Remote Access VPN Server to which you want to connect, as given to you by the network administrator.
2. To allow the VPN site to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the VPN site.
3. Click Next.

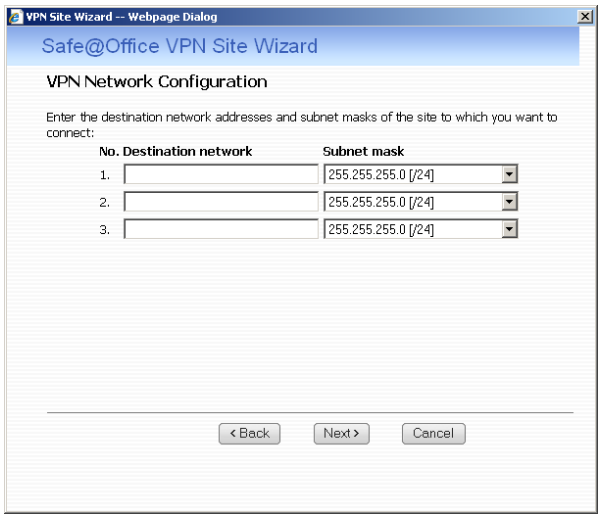
The VPN Network Configuration dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Network Configuration
How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.
Download Configuration:
Obtain the network configuration by downloading it from the site.
Specify Configuration:
Enter the network configuration manually.
Route All Traffic:
All network traffic will be routed via this site (Including Internet traffic)
< Back
Next >
Cancel

4. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 633.
5. Click Next.

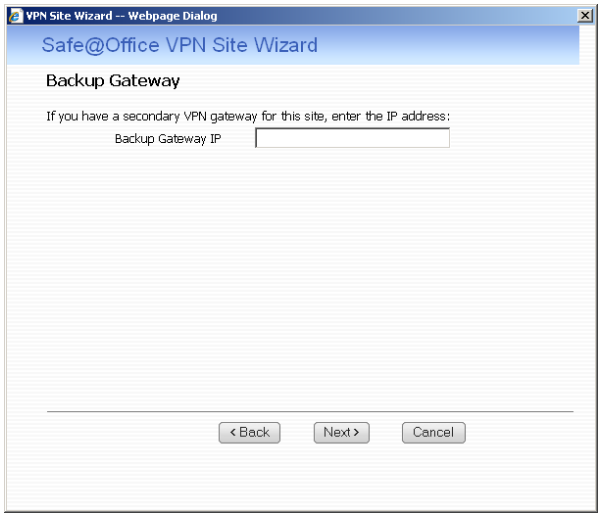
   The following things happen in the order below:

- If you chose Specify Configuration, a second VPN Network Configuration dialog box appears.



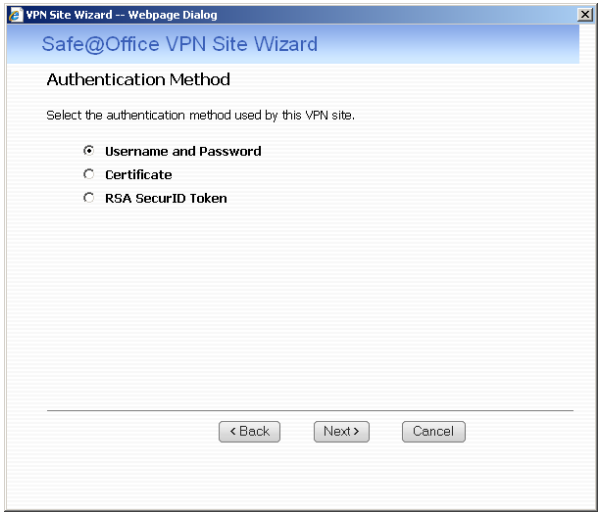
Complete the fields using the information in ***VPN Network Configuration Fields*** on page 633 and click Next.

- If you chose Specify Configuration or Route All Traffic, the Backup Gateway dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Backup Gateway
If you have a secondary VPN gateway for this site, enter the IP address:
Backup Gateway IP
< Back
Next >
Cancel

In the Backup Gateway IP field, type the name of the VPN site to use if the primary VPN site fails, and then click Next.

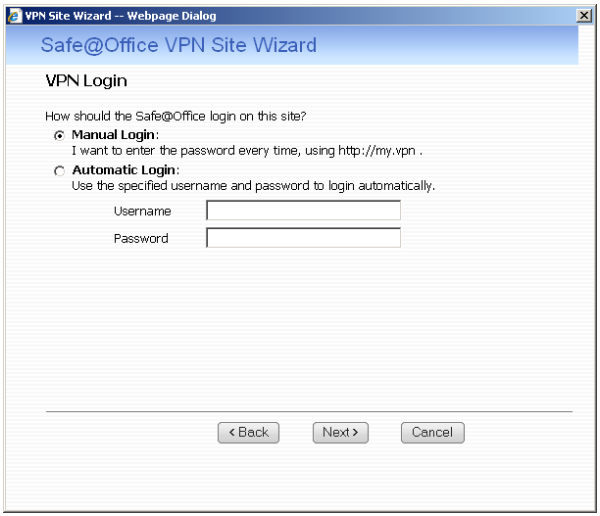
- The Authentication Method dialog box appears.



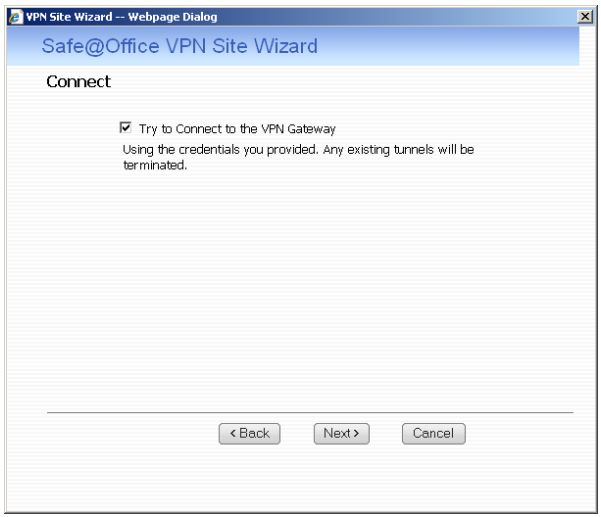
6. Complete the fields using the information in ***Authentication Methods Fields*** on page 635.
7. Click Next.

Username and Password Authentication Method

If you selected Username and Password, the VPN Login dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Login
How should the Safe@Office login on this site?
Manual Login:
I want to enter the password every time, using http://my.vpn .
Automatic Login:
Use the specified username and password to login automatically.
Username
Password
< Back
Next >
Cancel

1. Complete the fields using the information in ***VPN Login Fields*** on page 635.
2. Click Next.
   - If you selected Automatic Login, the Connect dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Connect
Try to Connect to the VPN Gateway
Using the credentials you provided. Any existing tunnels will be terminated.
< Back
Next >
Cancel

Do the following:

1) To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

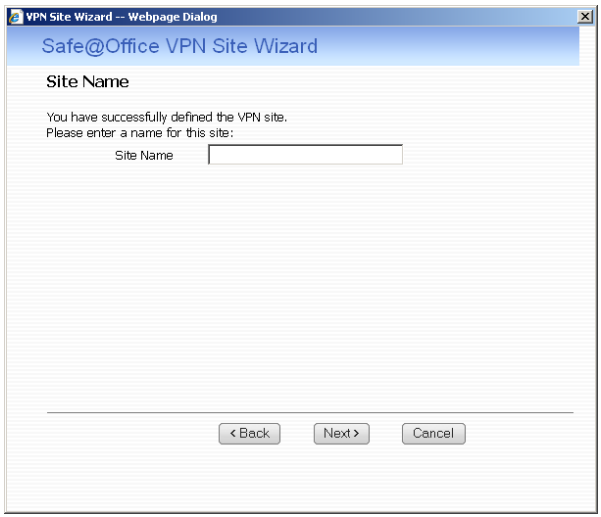
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

2) Click **Next**.

   If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.

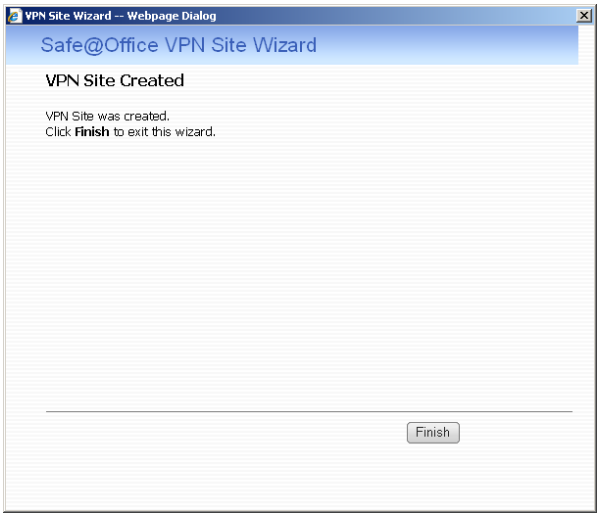

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Site Name
You have successfully defined the VPN site.
Please enter a name for this site:
Site Name
< Back
Next >
Cancel

3. Enter a name for the VPN site.

   You may choose any name.

4. Click **Next**.

The VPN Site Created screen appears.

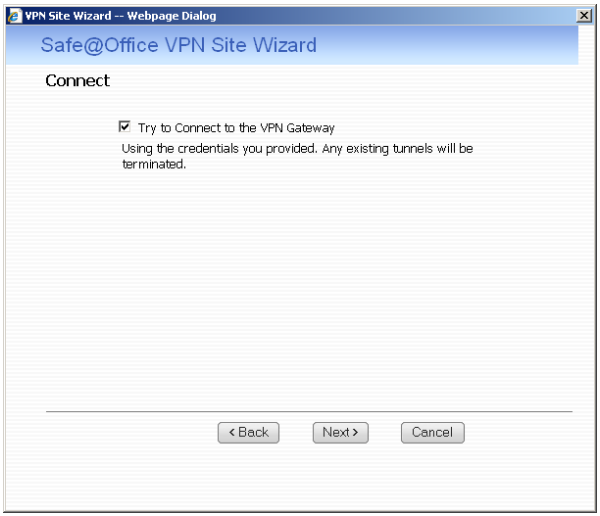

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Site Created
VPN Site was created.
Click Finish to exit this wizard.
Finish

5. Click Finish.

   The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Certificate Authentication Method

If you selected Certificate, the Connect dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Connect
Try to Connect to the VPN Gateway
Using the credentials you provided. Any existing tunnels will be terminated.
< Back
Next >
Cancel

1. To try to connect to the Remote Access VPN Server, select the Try to Connect to the VPN Gateway check box.

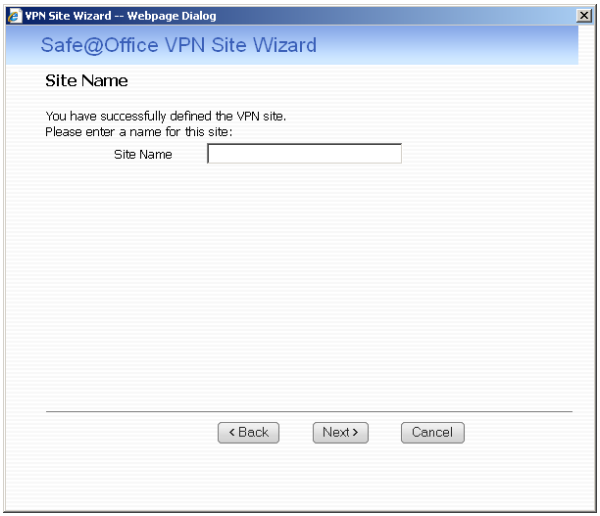
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

2. Click Next.

   If you selected Try to Connect to the VPN Gateway, the Connecting... screen appears, and then the Contacting VPN Site screen appears.

The Site Name dialog box appears.

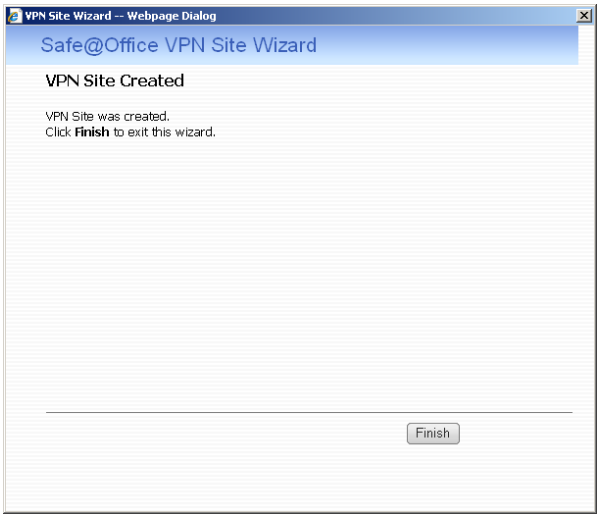

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Site Name
You have successfully defined the VPN site.
Please enter a name for this site:
Site Name
< Back
Next >
Cancel

3. Enter a name for the VPN site.

   You may choose any name.

4. Click Next.

   The VPN Site Created screen appears.

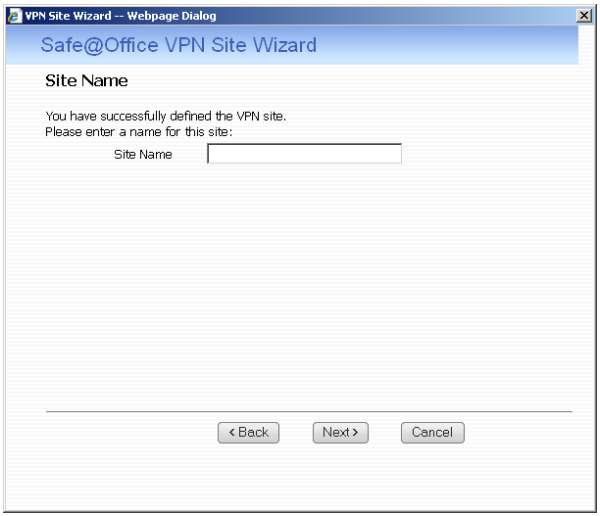

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Site Created
VPN Site was created.
Click Finish to exit this wizard.
Finish

5. Click Finish.

   The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

RSA SecurID Authentication Method

If you selected RSA SecurID, the Site Name dialog box appears.

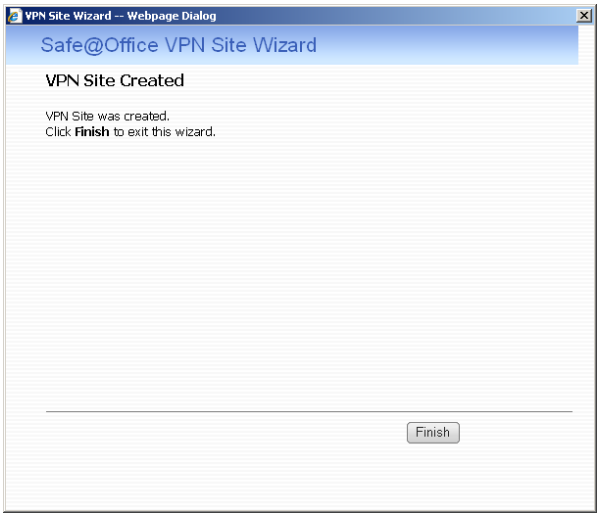

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Site Name
You have successfully defined the VPN site.
Please enter a name for this site:
Site Name
< Back
Next >
Cancel

1. Enter a name for the VPN site.

   You may choose any name.

2. Click Next.

The VPN Site Created screen appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Site Created
VPN Site was created.
Click Finish to exit this wizard.
Finish

3. Click Finish.

   The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Table 130: VPN Network Configuration Fields

In this field...	Do this...
Download Configuration	Click this option to obtain the network configuration by downloading it from the VPN site. This option will automatically configure your VPN settings, by downloading the network topology definition from the Remote Access VPN Server. Note: Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Safe@Office Site-to-Site VPN Gateway.

In this field...	Do this...
Specify Configuration	Click this option to provide the network configuration manually.
Route All Traffic	Click this option to route all network traffic through the VPN site. For example, if your VPN consists of a central office and a number of remote offices, and the remote offices are only allowed to access Internet resources through the central office, you can choose to route all traffic from the remote offices through the central office. Note: You can only configure one VPN site to route all traffic.
Route Based VPN	Click this option to create a virtual tunnel interface (VTI) for this site, so that it can participate in a route-based VPN. Route-based VPNs allow routing connections over VPN tunnels, so that remote VPN sites can participate in dynamic or static routing schemes. This improves network and VPN management efficiency for large networks. For constantly changing networks, it is recommended to use a route-based VPN combined with OSPF dynamic routing. This enables you to make frequent changes to the network topology, such as adding an internal network, without having to reconfigure static routes. OSPF is enabled using CLI. For information on using CLI, see ***Controlling the Appliance via the Command Line*** on page 711. For information on the relevant commands for OSPF, refer to the *Embedded NGX CLI Reference Guide*. This option is only available when configuring a Site-to-Site VPN gateway.
Destination network	Type up to three destination network addresses at the VPN site to which you want to connect.

In this field…	Do this…
Subnet mask	Select the subnet masks for the destination network addresses. Note: Obtain the destination networks and subnet masks from the VPN site's system administrator.

Table 131: Authentication Methods Fields

In this field…	Do this…
Username and Password	Select this option to use a user name and password for VPN authentication. In the next step, you can specify whether you want to log in to the VPN site automatically or manually.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 659 for more information about certificates and instructions on how to install a certificate.)
RSA SecurID Token	Select this option to use an RSA SecurID token for VPN authentication. When authenticating to the VPN site, you must enter a four-digit PIN code and the SecurID passcode shown in your SecurID token's display. The RSA SecurID token generates a new passcode every minute. SecurID is only supported in Remote Access manual login mode.

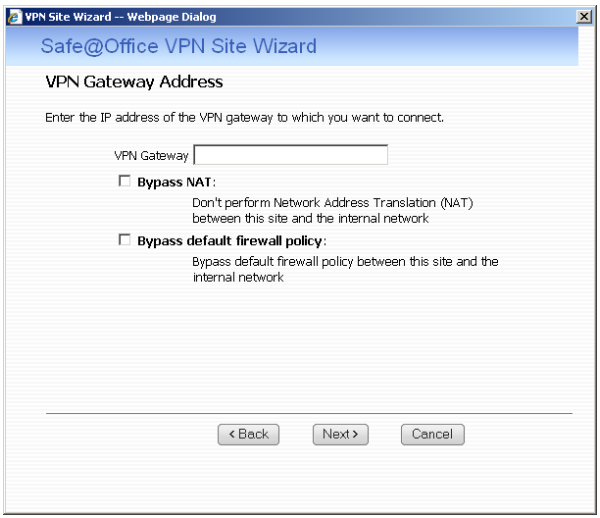
Table 132: VPN Login Fields

In this field…	Do this…
Manual Login	Click this option to configure the site for Manual Login. Manual Login connects only your computer to the VPN site, and only when

In this field...	Do this...
	the appropriate user name and password have been entered. For further information on Automatic and Manual Login, see, ***Logging in to a VPN Site*** on page 655.
Automatic Login	Click this option to enable the Safe@Office appliance to log in to the VPN site automatically. You must then fill in the Username and Password fields. Automatic Login provides all the computers on your internal network with constant access to the VPN site. For further information on Automatic and Manual Login, see ***Logging in to a VPN Site*** on page 655.
Username	Type the user name to be used for logging in to the VPN site.
Password	Type the password to be used for logging in to the VPN site.

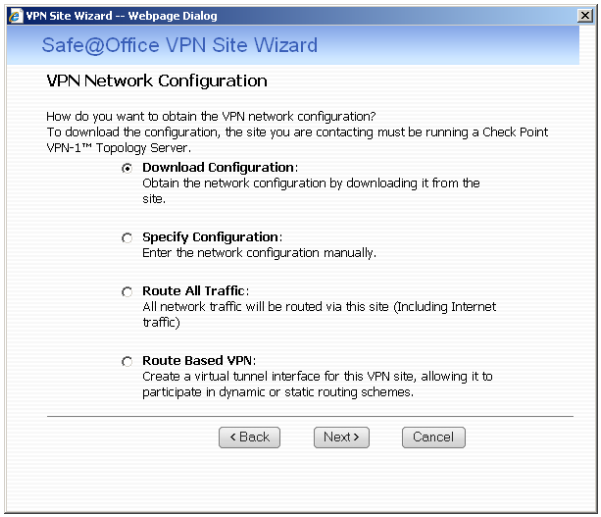
Configuring a Site-to-Site VPN Gateway

If you selected Site-to-Site VPN, the VPN Gateway Address dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Gateway Address
Enter the IP address of the VPN gateway to which you want to connect.
VPN Gateway
Bypass NAT:
Don't perform Network Address Translation (NAT) between this site and the internal network
Bypass default firewall policy:
Bypass default firewall policy between this site and the internal network
< Back
Next >
Cancel

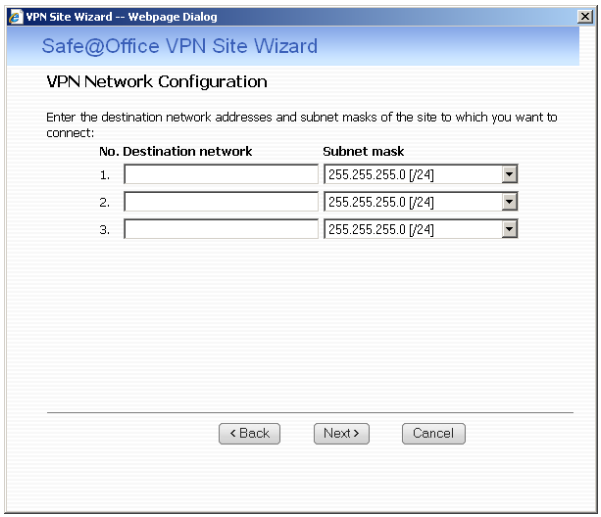
1. Complete the fields using the information in ***VPN Gateway Address Fields*** on page 650.
2. Click Next.

   The VPN Network Configuration dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
VPN Network Configuration
How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.
Download Configuration:
Obtain the network configuration by downloading it from the site.
Specify Configuration:
Enter the network configuration manually.
Route All Traffic:
All network traffic will be routed via this site (Including Internet traffic)
Route Based VPN:
Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.
< Back
Next >
Cancel

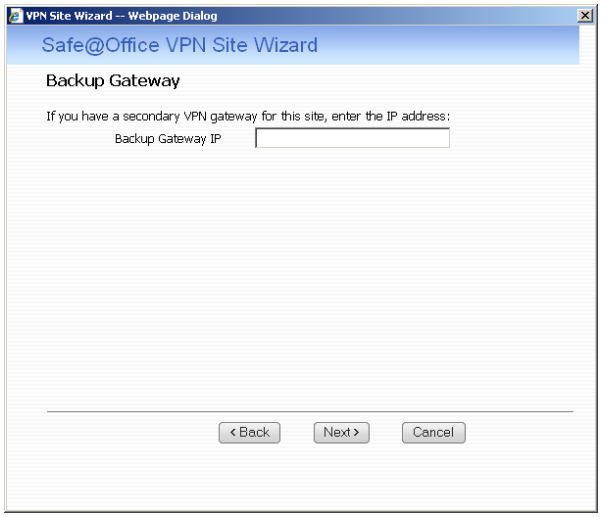
3. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 633.
4. Click Next.

- If you chose Specify Configuration, a second VPN Network Configuration dialog box appears.



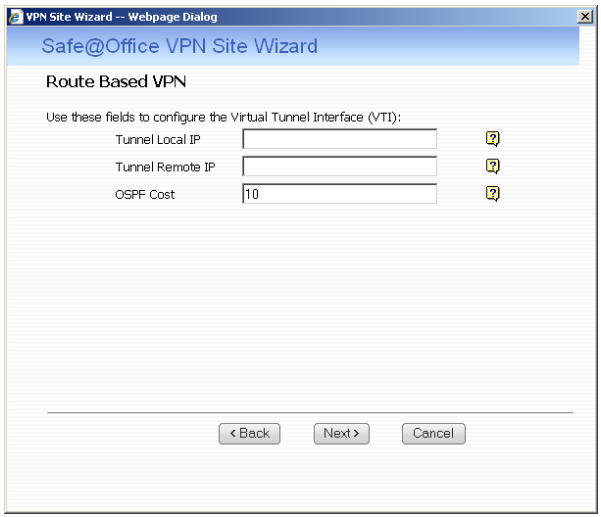
Complete the fields using the information in ***VPN Network Configuration Fields*** on page 633, and then click Next.

- If you chose Specify Configuration or Route All Traffic, the Backup Gateway dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Backup Gateway
If you have a secondary VPN gateway for this site, enter the IP address:
Backup Gateway IP
< Back
Next >
Cancel

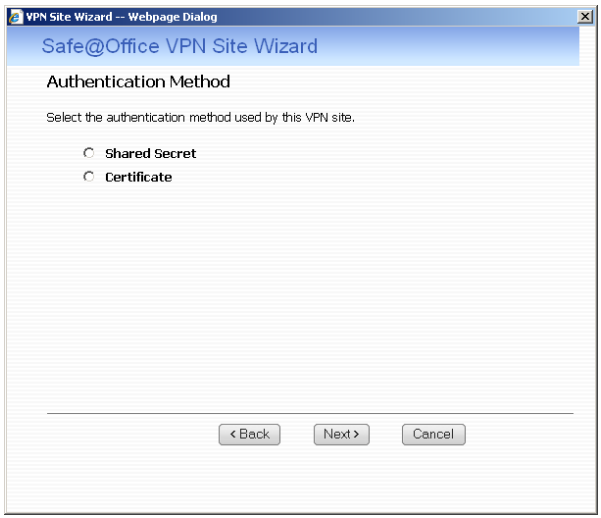
In the Backup Gateway IP field, type the name of the VPN site to use if the primary VPN site fails, and then click Next.

- If you chose Route Based VPN, the Route Based VPN dialog box appears.



Complete the fields using the information in ***Route Based VPN Fields*** on page 650, and then click Next.

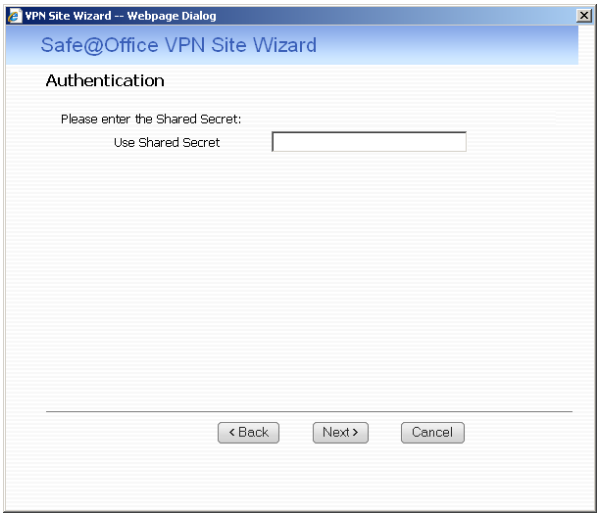
- The Authentication Method dialog box appears.



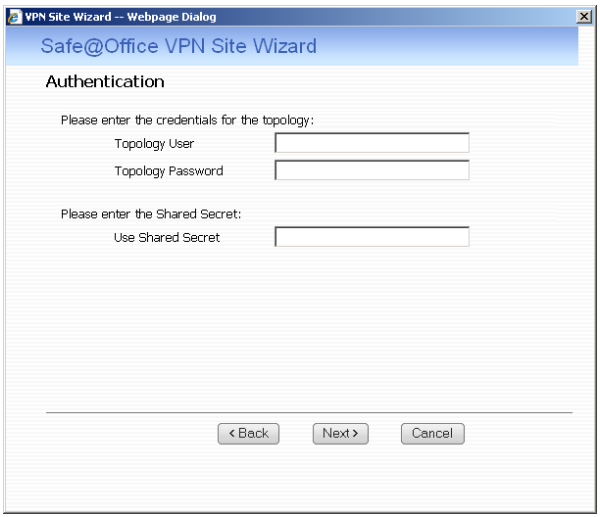
5. Complete the fields using the information in ***Authentication Methods Fields*** on page 651.
6. Click Next.

Shared Secret Authentication Method

If you selected Shared Secret, the Authentication dialog box appears.



If you chose Download Configuration, the dialog box contains additional fields.



1. Complete the fields using the information in ***VPN Authentication Fields*** on page 651 and click Next.

The Security Methods dialog box appears.

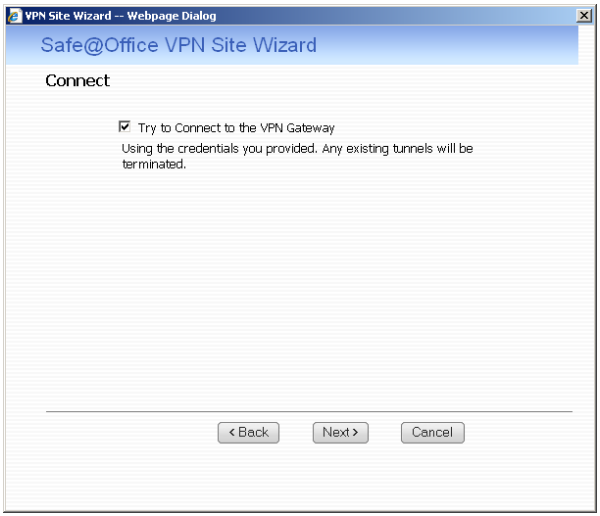
VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Security Methods
Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.
Show Advanced Settings
Phase 1
Security Methods
Automatic
Phase 2
Security Methods
Automatic
< Back
Next >
Cancel

2. To configure advanced security settings, click Show Advanced Settings.

   New fields appear.

3. Complete the fields using the information in ***Security Methods Fields*** on page 652 and click Next.

The Connect dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Connect
Try to Connect to the VPN Gateway
Using the credentials you provided. Any existing tunnels will be terminated.
< Back
Next >
Cancel

4. To try to connect to the Remote Access VPN Server, select the Try to Connect to the VPN Gateway check box.

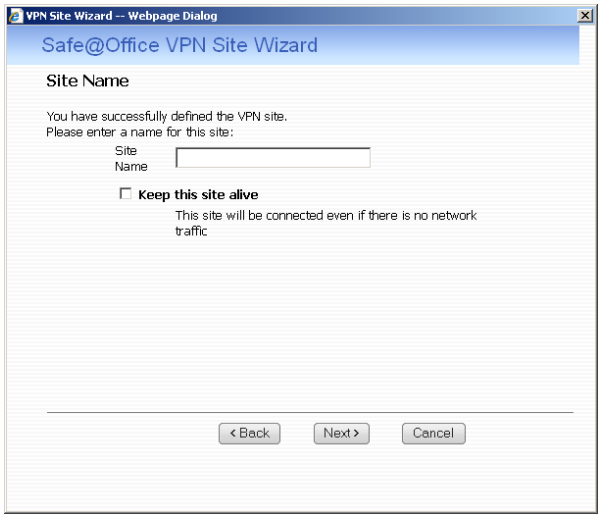
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

5. Click Next.

   - If you selected Try to Connect to the VPN Gateway, the Connecting... screen appears, and then the Contacting VPN Site screen appears.

- The Site Name dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Site Name
You have successfully defined the VPN site.
Please enter a name for this site:
Site Name
Keep this site alive
This site will be connected even if there is no network traffic
< Back
Next >
Cancel

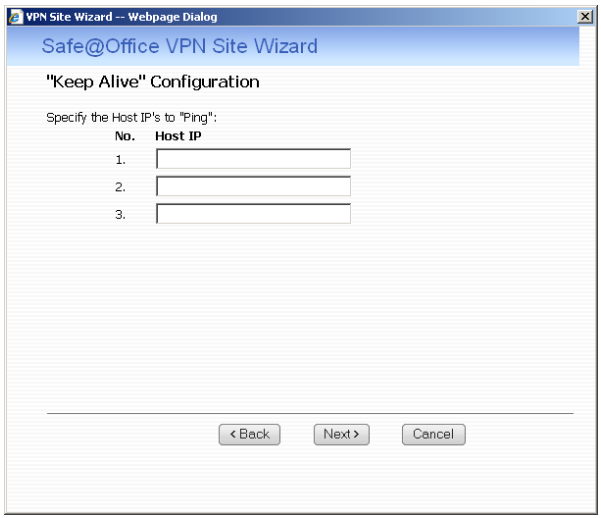
6. Type a name for the VPN site.

   You may choose any name.

7. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select Keep this site alive.

8. Click Next.

- If you selected Keep this site alive, and previously you chose Download Configuration, the "Keep Alive" Configuration dialog box appears.



Do the following:

1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.
2) Click Next.

- The VPN Site Created screen appears.

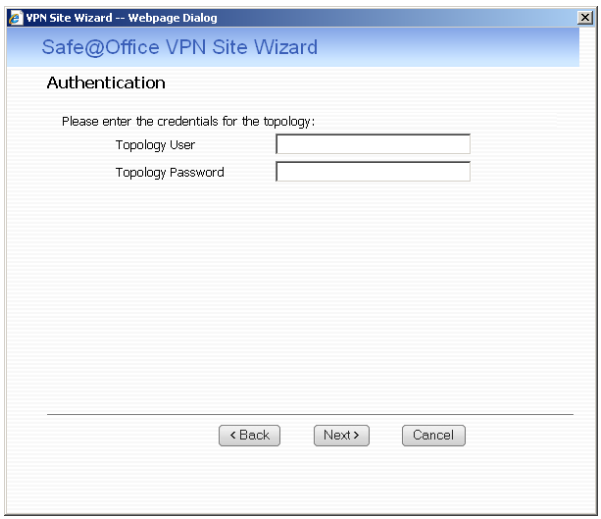
9. Click Finish.

The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Certificate Authentication Method

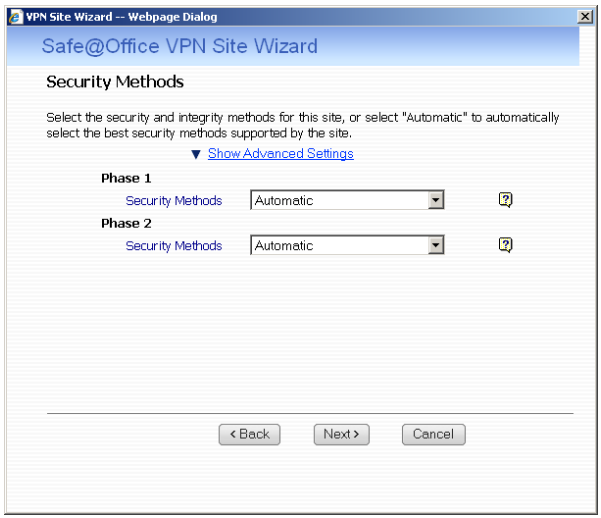
If you selected Certificate, the following things happen:

- If you chose Download Configuration, the Authentication dialog box appears.



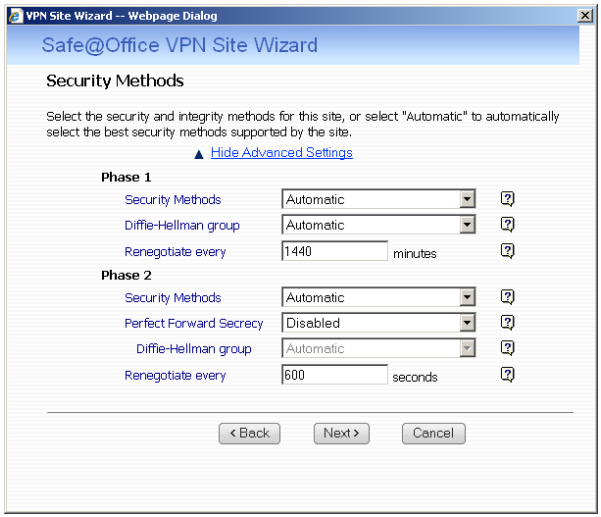
Complete the fields using the information in ***VPN Authentication Fields*** on page 651 and click Next.

- The Security Methods dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Security Methods
Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.
▼ Show Advanced Settings
Phase 1
Security Methods
Automatic
Phase 2
Security Methods
Automatic
< Back
Next >
Cancel

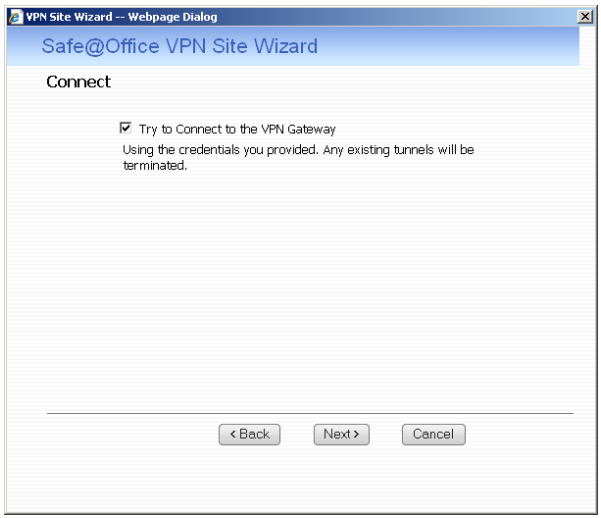
1. To configure advanced security settings, click Show Advanced Settings.

   New fields appear.



2. Complete the fields using the information in ***Security Methods Fields*** on page 652 and click Next.

   The Connect dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Connect
Try to Connect to the VPN Gateway
Using the credentials you provided. Any existing tunnels will be terminated.
< Back
Next >
Cancel

3. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

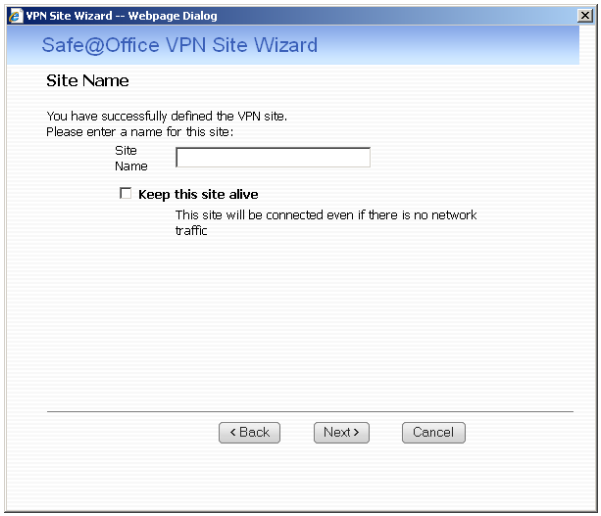
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

4. Click **Next**.

   - If you selected **Try to Connect to the VPN Gateway**, the following things happen:

     The **Connecting**... screen appears.
   - The **Contacting VPN Site** screen appears.
   - The **Site Name** dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Site Name
You have successfully defined the VPN site.
Please enter a name for this site:
Site Name
Keep this site alive
This site will be connected even if there is no network traffic
< Back
Next >
Cancel

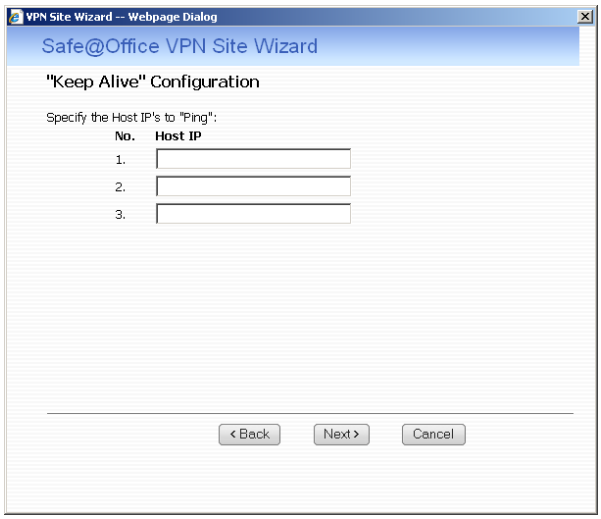
5. Enter a name for the VPN site.

   You may choose any name.

6. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select **Keep this site alive**.

7. Click **Next**.

- If you selected Keep this site alive, and previously you chose Download Configuration, the "Keep Alive" Configuration dialog box appears.



Do the following:

1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.
2) Click Next.

- The VPN Site Created screen appears.

8. Click Finish.

The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Table 133: VPN Gateway Address Fields

In this field…	Do this…
Gateway Address	Type the IP address of the Site-to-Site VPN Gateway to which you want to connect, as given to you by the network administrator.
Bypass NAT	Select this option to allow the VPN site to bypass NAT when connecting to your internal network. This option is selected by default.
Bypass default firewall policy	Select this option to allow the VPN site to bypass the default firewall policy and access your internal network without restriction. User-defined rules will still apply to the VPN site.

Table 134: Route Based VPN Fields

In this field…	Do this…
Tunnel Local IP	Type a local IP address for this end of the VPN tunnel.
Tunnel Remote IP	Type the IP address of the remote end of the VPN tunnel.
OSPF Cost	Type the cost of this link for dynamic routing purposes. The default value is 10. If OSPF is not enabled, this setting is not used. OSPF is enabled using the Safe@Office command line interface (CLI). For information on using CLI, see ***Controlling the Appliance via the Command Line*** on page 711. For information on the relevant commands for OSPF, refer to the *Embedded NGX CLI Reference Guide*.

Table 135: Authentication Methods Fields

In this field…	Do this…
Shared Secret	Select this option to use a shared secret for VPN authentication. A shared secret is a string used to identify VPN sites to each other.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 659 for more information about certificates and instructions on how to install a certificate.)

Table 136: VPN Authentication Fields

In this field…	Do this…
Topology User	Type the topology user's user name.
Topology Password	Type the topology user's password.
Use Shared Secret	Type the shared secret to use for secure communications with the VPN site. This shared secret is a string used to identify the VPN sites to each other. The secret can contain spaces and special characters.

Table 137: Security Methods Fields

In this field…	Do this…
Phase 1	
Security Methods	Select the encryption and integrity algorithm to use for IKE negotiations: • Automatic. The Safe@Office appliance automatically selects the best security methods supported by the site. This is the default. • A specific algorithm
Diffie-Hellman group	Select the Diffie-Hellman group to use: • Automatic. The Safe@Office appliance automatically selects a group. This is the default. • A specific group A group with more bits ensures a stronger key but lowers performance.
Renegotiate every	Type the interval in minutes between IKE Phase-1 key negotiations. This is the *IKE Phase-1 SA lifetime*. A shorter interval ensures higher security, but impacts heavily on performance. Therefore, it is recommended to keep the SA lifetime around its default value. The default value is 1440 minutes (one day).
Phase 2	
Security Methods	Select the encryption and integrity algorithm to use for VPN traffic: • Automatic. The Safe@Office appliance automatically selects the best security methods supported by the site. This is the default. • A specific algorithm

In this field...	Do this...
Perfect Forward Secrecy	Specify whether to enable Perfect Forward Secrecy (PFS), by selecting one of the following: • Enabled. PFS is enabled. The Diffie-Hellman group field is enabled. • Disabled. PFS is disabled. This is the default. Enabling PFS will generate a new Diffie-Hellman key during IKE Phase 2 and renew the key for each key exchange. PFS increases security but lowers performance. It is recommended to enable PFS only in situations where extreme security is required.
Diffie-Hellman group	Select the Diffie-Hellman group to use: • Automatic. The Safe@Office appliance automatically selects a group. This is the default. • A specific group A group with more bits ensures a stronger key but lowers performance.
Renegotiate every	Type the interval in seconds between IPSec SA key negotiations. This is the *IKE Phase-2 SA lifetime*. A shorter interval ensures higher security. The default value is 3600 seconds (one hour).

Viewing and Deleting VPN Sites

500 1000N

To view or delete a VPN site

1. Click VPN in the main menu, and click the VPN Sites tab.

   The VPN Sites page appears, with a list of all VPN sites.

2. To delete a VPN site, do the following.

   a. In the desired VPN site's row, click the Erase icon.
   A confirmation message appears.

   b. Click OK.
   The VPN site is deleted.

Enabling/Disabling a VPN Site

500 1000N

You can only connect to VPN sites that are enabled.

To enable/disable a VPN site

1. Click VPN in the main menu, and click the VPN Sites tab.

   The VPN Sites page appears, with a list of VPN sites.

2. To enable a VPN site, do the following:

   a. Click the icon in the desired VPN site's row.
   A confirmation message appears.

   b. Click OK.

   The icon changes to , and the VPN site is enabled.

3. To disable a VPN site, do the following:

Note: Disabling a VPN site eliminates the tunnel and erases the network topology.

a. Click the icon in the desired VPN site's row.
   A confirmation message appears.
b. Click OK.
   The icon changes to , and the VPN site is disabled.

Logging in to a Remote Access VPN Site

500 1000N

You need to manually log in to Remote Access VPN Servers configured for Manual Login. You do not need to manually log in to a Remote Access VPN Server configured for Automatic Login or a Site-to-Site VPN Gateway: all the computers on your network have constant access to it.

Manual Login can be done through either the Safe@Office Portal or the my.vpn page. When you log in and traffic is sent to the VPN site, a VPN tunnel is established. Only the computer from which you logged in can use the tunnel. To share the tunnel with other computers in your home network, you must log in to the VPN site from those computers, using the same user name and password.

Note: You must use a single user name and password for each VPN destination gateway.

Logging in through the Safe@Office Portal

500 1000N

Note: You can only log in to sites that are configured for Manual Login.

To manually log in to a VPN site through the Safe@Office Portal

1. Click VPN in the main menu, and click the VPN Sites tab.

   The VPN Sites page appears.

2. Next to the desired VPN site, click Login.

   The VPN Status dialog box appears.

3. Type your user name and password in the appropriate fields.
4. Click Login.
   - If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.
   - If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.

     Once the Safe@Office appliance has finished connecting, the dialog box displays "Connected".
   - The VPN Status dialog box remains open until you manually log out of the VPN site.

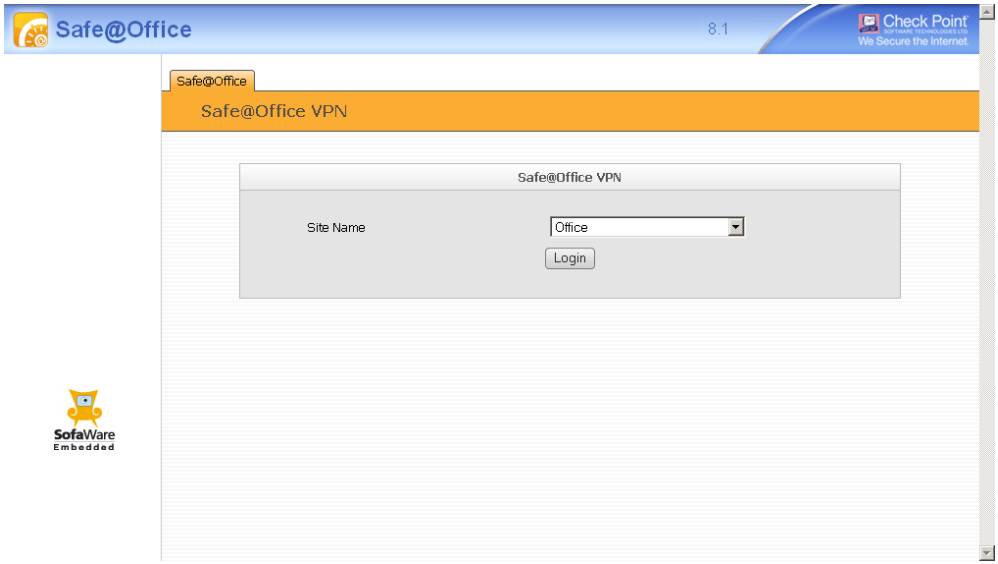
Logging in through the my.vpn page

500 1000N

To manually log in to a VPN site through the my.vpn page

1. Direct your Web browser to http://my.vpn

   The VPN Login screen appears.



2. In the Site Name list, select the site to which you want to log in.
3. Enter your user name and password in the appropriate fields.
4. Click Login.
   - If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.
   - If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.
   - The VPN Login Status box appears. The Status field tracks the connection's progress.

- Once the Safe@Office appliance has finished connecting, the Status field changes to “Connected”.
- The VPN Login Status box remains open until you manually log out of the VPN site.

Logging Out of a Remote Access VPN Site

500 1000N

You can manually log out of a VPN site, if it is a Remote Access VPN site configured for Manual Login.

To log out of a VPN site

- In the VPN Login Status box, click Logout.

  All open tunnels from the Safe@Office appliance to the VPN site are closed, and the VPN Login Status box closes.

Note: Closing the browser or dismissing the VPN Login Status box will also terminate the VPN session within a short time.

Using Certificates

500 1000N

A digital certificate is a secure means of authenticating the Safe@Office appliance to other Site-to-Site VPN Gateways. The certificate is issued by the Certificate Authority (CA) to entities such as gateways, users, or computers. The entity then uses the certificate to identify itself and provide verifiable information.

For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

The certificate also includes a fingerprint, a unique text used to identify the certificate. You can email your certificate's fingerprint to the remote user. Upon connecting to the

Safe@Office VPN Server for the first time, the entity should check that the VPN peer's fingerprint displayed in the SecuRemote/SecureClient VPN Client is identical to the fingerprint received.

The Safe@Office appliance supports certificates encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format.

Installing a Certificate

500 1000N

The Safe@Office appliance enables you to install PKCS#12 certificates in the following ways:

- By generating a self-signed certificate.

  See ***Generating a Self-Signed Certificate*** on page 660.

- By importing a certificate.

  The PKCS#12 file you import must have a ".p12" file extension. If you do not have such a PKCS#12 file, obtain one from your network security administrator.

  See ***Importing a Certificate*** on page 664.

Note: To use certificates authentication, each Safe@Office appliance should have a unique certificate. Do not use the same certificate for more than one gateway.

Note: If your Safe@Office appliance is centrally managed, a certificate is automatically generated and downloaded to your appliance. In this case, there is no need to generate a self-signed certificate.

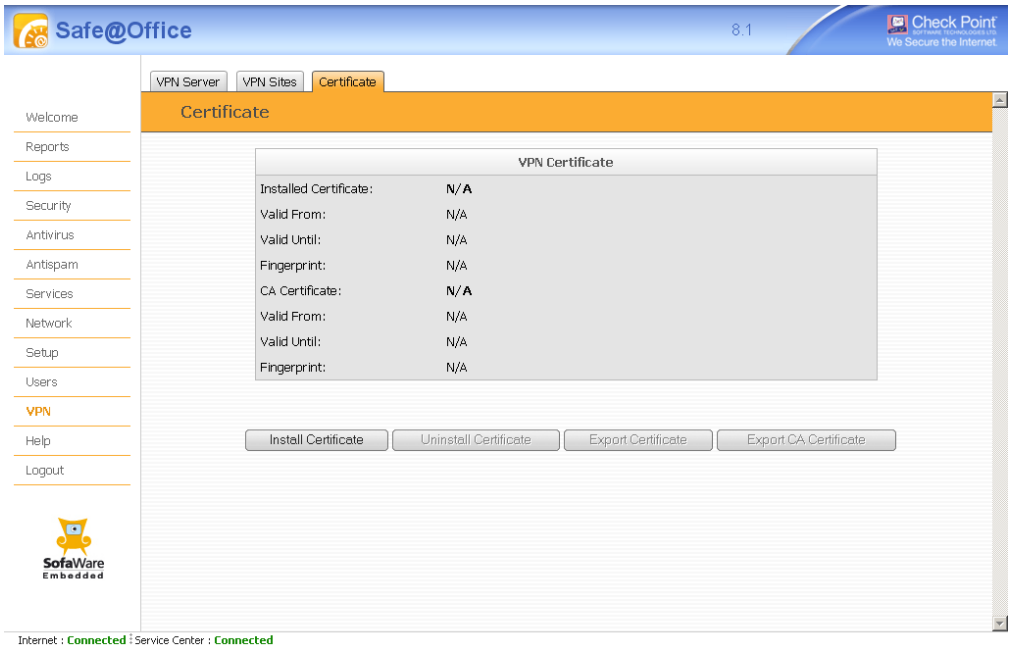
Generating a Self-Signed Certificate

500 1000N

To generate a self-signed certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.



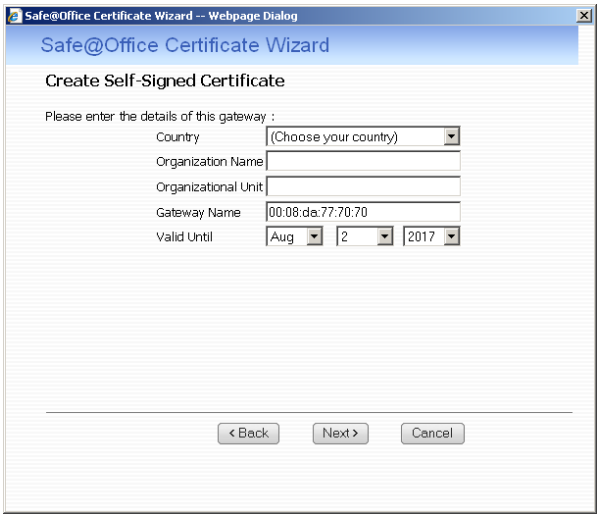
2. Click Install Certificate.

The Safe@Office Certificate Wizard opens, with the Certificate Wizard dialog box displayed.

Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard
Welcome to the Certificate Wizard
A digital certificate is a secure means of authenticating the Safe@Office gateway to other gateways. You can install a certificate in the following ways:
Generate a self-signed security certificate for this gateway
Import a security certificate in PKCS#12 format
Next >
Cancel

3. Click Generate a self-signed security certificate for this gateway.

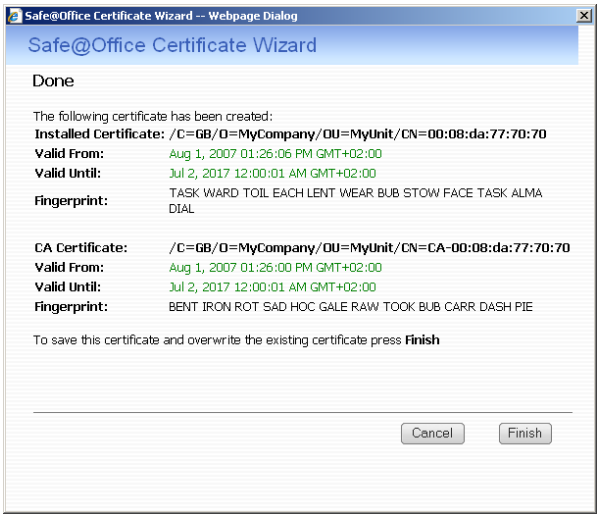
   The Create Self-Signed Certificate dialog box appears.



4. Complete the fields using the information in the following table.
5. Click Next.

The Safe@Office appliance generates the certificate. This may take a few seconds.

The Done dialog box appears, displaying the certificate's details.


Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard
Done
The following certificate has been created:
Installed Certificate: /C=GB/O=MyCompany/OU=MyUnit/CN=00:08:da:77:70:70
Valid From: Aug 1, 2007 01:26:06 PM GMT+02:00
Valid Until: Jul 2, 2017 12:00:01 AM GMT+02:00
Fingerprint: TASK WARD TOIL EACH LENT WEAR BUB STOW FACE TASK ALMA DIAL
CA Certificate: /C=GB/O=MyCompany/OU=MyUnit/CN=CA-00:08:da:77:70:70
Valid From: Aug 1, 2007 01:26:00 PM GMT+02:00
Valid Until: Jul 2, 2017 12:00:01 AM GMT+02:00
Fingerprint: BENT IRON ROT SAD HOC GALE RAW TOOK BUB CARR DASH PIE
To save this certificate and overwrite the existing certificate press Finish
Cancel
Finish

6. Click Finish.

The Safe@Office appliance installs the certificate. If a certificate is already installed, it is overwritten.

The Certificate Wizard closes.

The Certificates page displays the following information:

- The gateway's certificate
- The gateway's name
- The gateway certificate's fingerprint
- The CA's certificate
- The name of the CA that issued the certificate (in this case, the Safe@Office gateway)
- The CA certificate's fingerprint

- The starting and ending dates between which the gateway's certificate and the CA's certificate are valid

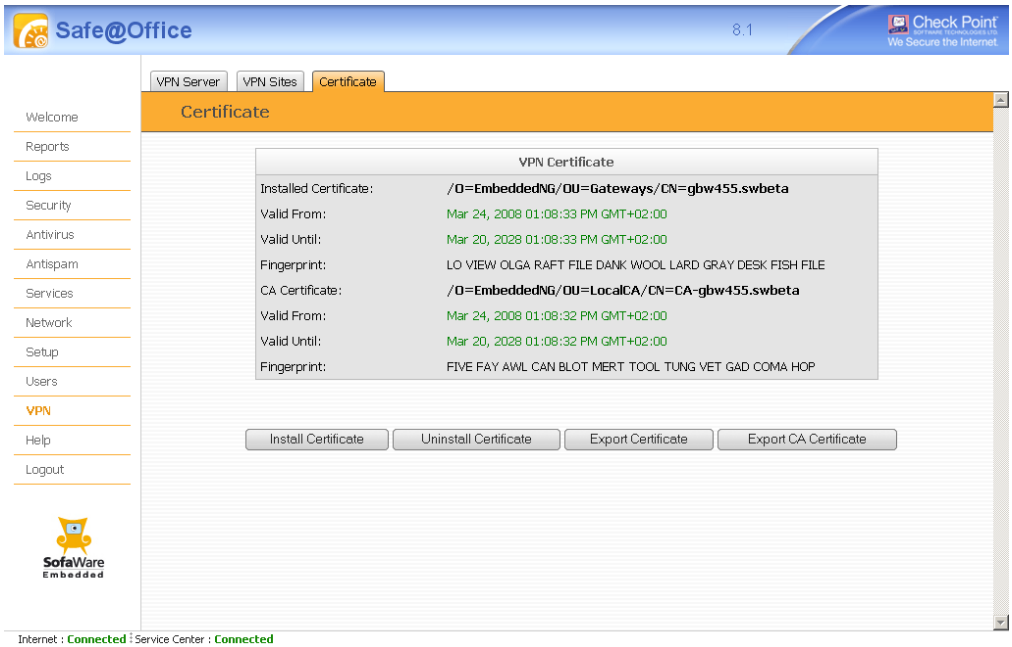


Table 138: Certificate Fields

In this field…	Do this…
Country	Select your country from the drop-down list.
Organization Name	Type the name of your organization.
Organizational Unit	Type the name of your division.
Gateway Name	Type the gateway's name. This name will appear on the certificate, and will be visible to remote users inspecting the certificate. This field is filled in automatically with the gateway's MAC address. If desired, you can change this to a more descriptive name.
Valid Until	Use the drop-down lists to specify the month, day, and year when this certificate should expire. Note: You must renew the certificate when it expires.

Importing a Certificate

500 1000N

To install a certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.

2. Click Install Certificate.

   The Safe@Office Certificate Wizard opens, with the Certificate Wizard dialog box displayed.

3. Click Import a security certificate in PKCS#12 format.

The Import Certificate dialog box appears.

Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard
Import Certificate
To install a certificate (which will overwrite any existing installed one):
1. Obtain the PKCS#12 Certificate file from your network security administrator
2. Click Browse... and select the Certificate file (with a p12 suffix)
3. Click Next
Browse...
< Back
Next >
Cancel

4. Click Browse to open a file browser from which to locate and select the file.

   The filename that you selected is displayed.

5. Click Next.

   The Import-Certificate Passphrase dialog box appears. This may take a few moments.

Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard
Import Certificate - Passphrase
Please enter the certificate passphrase, and click Next to view the certificate.
< Back
Next >
Cancel

6. Type the pass-phrase you received from the network security administrator.
7. Click Next.

   The Done dialog box appears, displaying the certificate's details.
8. Click Finish.

   The Safe@Office appliance installs the certificate. If a certificate is already installed, it is overwritten.

   The Certificate Wizard closes.

   The Certificates page displays the following information:

   - The gateway's certificate
   - The gateway's name
   - The gateway certificate's fingerprint
   - The CA's certificate
   - The name of the CA that issued the certificate
   - The CA certificate's fingerprint
   - The starting and ending dates between which the gateway's certificate and the CA's certificate are valid

Uninstalling a Certificate

500 1000N

If you uninstall the certificate, no certificate will exist on the Safe@Office appliance, and you will not be able to connect to the VPN if a certificate is required.

You cannot uninstall the certificate if there is a VPN site currently defined to use certificate authentication.

Note: If you want to replace a currently-installed certificate, there is no need to uninstall the certificate first. When you install the new certificate, the old certificate will be overwritten.

To uninstall a certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.

2. Click Uninstall.

   A confirmation message appears.

3. Click OK.

   The certificate is uninstalled.

   A success message appears.

4. Click OK.

Exporting Certificates

500 1000N

The Safe@Office appliance allows you to export the following certificates:

- The device certificate

  Exporting the device certificate is useful for backup purposes.

Note: If your Safe@Office appliance is centrally managed, there is no need to back up the device certificate, as it can be downloaded from the Service Center as needed.

- The device Certificate Authority (CA) certificate

  When using the Safe@Office EAP authenticator with WPA-Enterprise or 802.1x security protocols, you must export the device CA certificate and send it to clients that need to connect to the Safe@Office appliance. For information on the EAP authenticator, see ***Using the EAP Authenticator*** on page 433.

The certificates are exported in PKCS#12 format (that is, as a *.p12 file).

Exporting the Safe@Office Appliance Certificate

500 1000N

To export the Safe@Office appliance certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.
2. Click Export Certificate.

   A standard File Download dialog box appears.
3. Click Save.

   The Save As dialog box appears.
4. Browse to a destination directory of your choice.
5. Type a name for the certificate file and click Save.

The certificate is exported as a *.p12 file and saved to the specified directory.

Note: This file contains the gateway's private key, which is confidential and must not be passed to unauthorized users.

Exporting the CA Certificate

500 1000N

To export the CA certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.
2. Click Export CA Certificate.

   A standard File Download dialog box appears.
3. Click Save.

   The Save As dialog box appears.
4. Browse to a destination directory of your choice.
5. Type a name for the CA certificate file and click Save.

   The CA certificate is exported as a *.p12 file and saved to the specified directory.

Viewing VPN Tunnels

500 1000N

You can view a list of currently established VPN tunnels. VPN tunnels are created and closed as follows:

- Remote Access VPN sites configured for Automatic Login and Site-to-Site VPN Gateways

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site. The tunnel is closed when not in use for a period of time.

Note: Although the VPN tunnel is automatically closed, the site remains open, and if you attempt to communicate with the site, the tunnel will be reestablished.

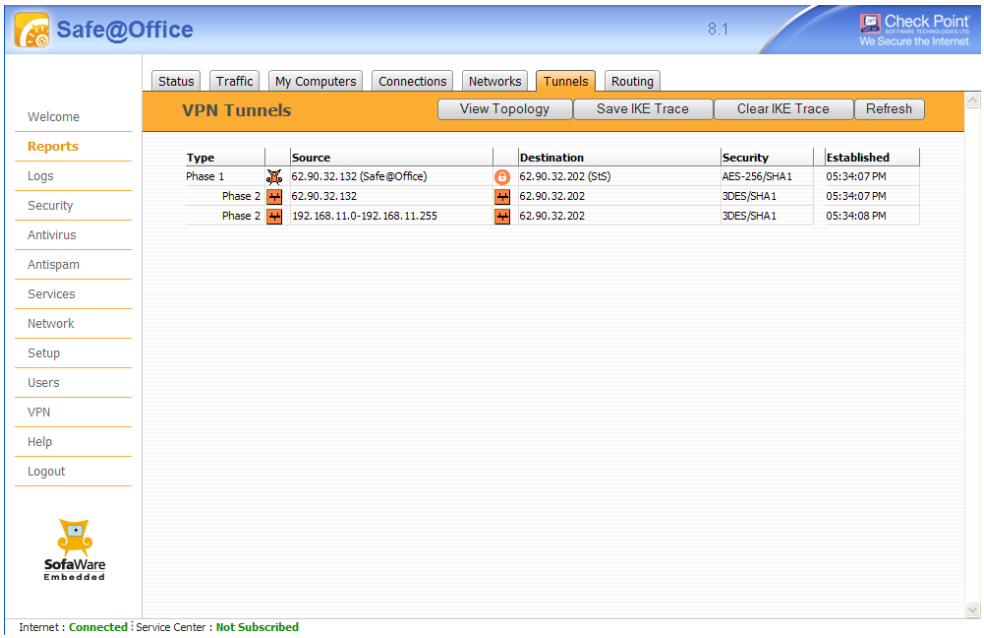
- Remote Access VPN sites configured for Manual Login

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site, *after you have manually logged in to the site*. All open tunnels connecting to the site are closed when you manually log out.

To view VPN tunnels

1. Click Reports in the main menu, and click the Tunnels tab.

The VPN Tunnels page appears with a table of open VPN tunnels.



The VPN Tunnels page includes the information described in the following table.

2. To resize a column, drag the relevant column divider right or left.
3. To refresh the table, click Refresh.

Table 139: VPN Tunnels Page Fields

This field...	Displays...
Type	The currently active security protocol (IPSEC).
Source	The IP address or address range of the entity from which the tunnel originates. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 672.

This field...	Displays...
Destination	The IP address or address range of the entity to which the tunnel is connected. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 672.
Security	The type of encryption used to secure the connection, and the type of Message Authentication Code (MAC) used to verify the integrity of the message. This information is presented in the following format: Encryption type/Authentication type. In addition, if IPSec compression is enabled for the tunnel, this field displays the icon. Note: All VPN settings are automatically negotiated between the two sites. The encryption and authentication schemes used for the connection are the strongest of those used at the two sites. Your Safe@Office appliance supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.
Established	The time at which the tunnel was established. This information is presented in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds

Table 140: VPN Tunnels Icons

This icon...	Represents...
	This gateway

This icon...	Represents...
	A network for which an IKE Phase-2 tunnel was negotiated
	A Remote Access VPN Server
	A Site-to-Site VPN Gateway
	A remote access VPN user
	An L2TP user

Viewing IKE Traces for VPN Connections

500 1000N

If you are experiencing VPN connection problems, you can save a trace of IKE (Internet Key Exchange) negotiations to a file, and then use the free IKE View tool to view the file.

The IKE View tool is available for the Windows platform.

Note: Before viewing IKE traces, it is recommended to do the following:

- The Safe@Office appliance stores traces for all recent IKE negotiations. If you want to view only new IKE trace data, clear all IKE trace data currently stored on the Safe@Office appliance.
- Close all existing VPN tunnels except for the problematic tunnel, so as to make it easier to locate the problematic tunnel's IKE negotiation trace in the exported file.

To clear all currently-stored IKE traces

1. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

2. Click Clear IKE Trace.

   All IKE trace data currently stored on the Safe@Office appliance is cleared.

To view the IKE trace for a connection

1. Establish a VPN tunnel to the VPN site with which you are experiencing connection problems.

   For information on when and how VPN tunnels are established, see ***Viewing VPN Tunnels*** on page 670.

2. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

3. Click Save IKE Trace.

   A standard File Download dialog box appears.

4. Click Save.

   The Save As dialog box appears.

5. Browse to a destination directory of your choice.

6. Type a name for the *.elg file and click Save.

   The *.elg file is created and saved to the specified directory. This file contains the IKE traces of all currently-established VPN tunnels.

7. Use the IKE View tool to open and view the *.elg file, or send the file to technical support.

Viewing VPN Topology

500 1000N

You can view the topology of VPN sites to which the Safe@Office appliance is currently connected.

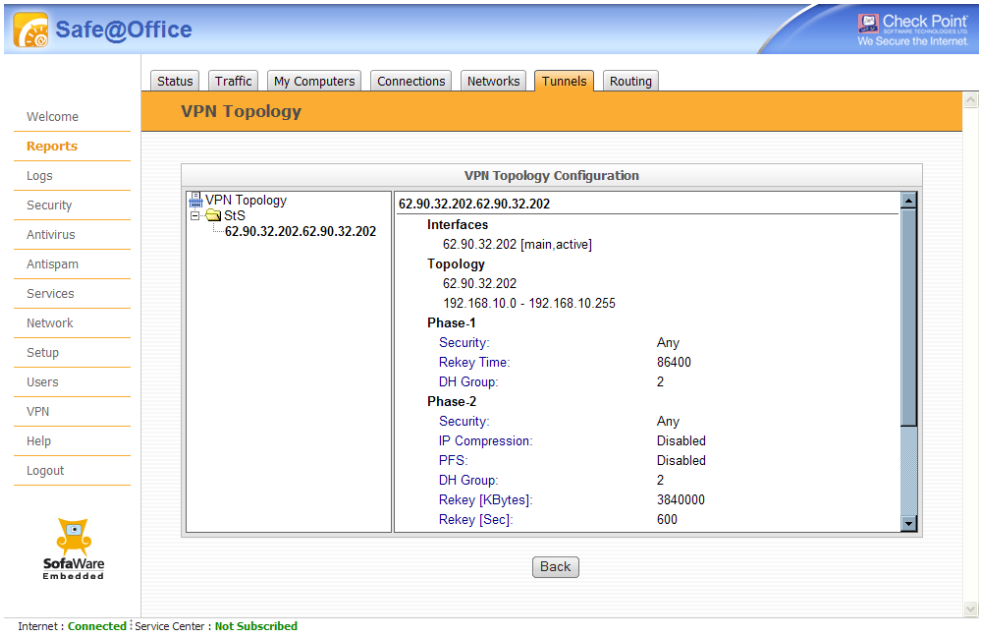
To view VPN topology

1. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

2. Click View Topology.

The VPN Topology page appears displaying a tree of VPN sites to which the appliance is connected.



3. To view topology information for a VPN site, in the tree, click the VPN site's name.

   The right pane displays the information described in the following table.

Table 141: VPN Topology Page Fields

This field...	Displays...
Split DNS	The VPN site's split DNS mappings. When split DNS is configured for a VPN site, certain domain suffixes are mapped to corporate DNS servers. This means that requests for these domain suffixes are sent to the specific DNS servers to which they are mapped, while all other requests are sent to the ISP's DNS servers. For example, a VPN site's split DNS mappings might indicate that all requests for the domain suffix ".acme.com" should be sent to the Acme company's corporate DNS servers.
Trusted CAs	A list of root CAs at the VPN site, whose certificates are trusted by this gateway.
Sub-CAs	A list of second-level CAs at the VPN site, which are signed by a trusted root CA.

Chapter 20

Managing Users

This chapter describes how to manage Safe@Office appliance users. You can define multiple users, set their passwords, and assign them various permissions.

This chapter includes the following topics:

Changing Your Login Credentials....677
Adding and Editing Users....680
Adding Quick Guest HotSpot Users....685
Viewing and Deleting Users....686
Setting Up Remote VPN Access for Users....687
Using RADIUS Authentication....688
Configuring RADIUS Attributes....694

Changing Your Login Credentials

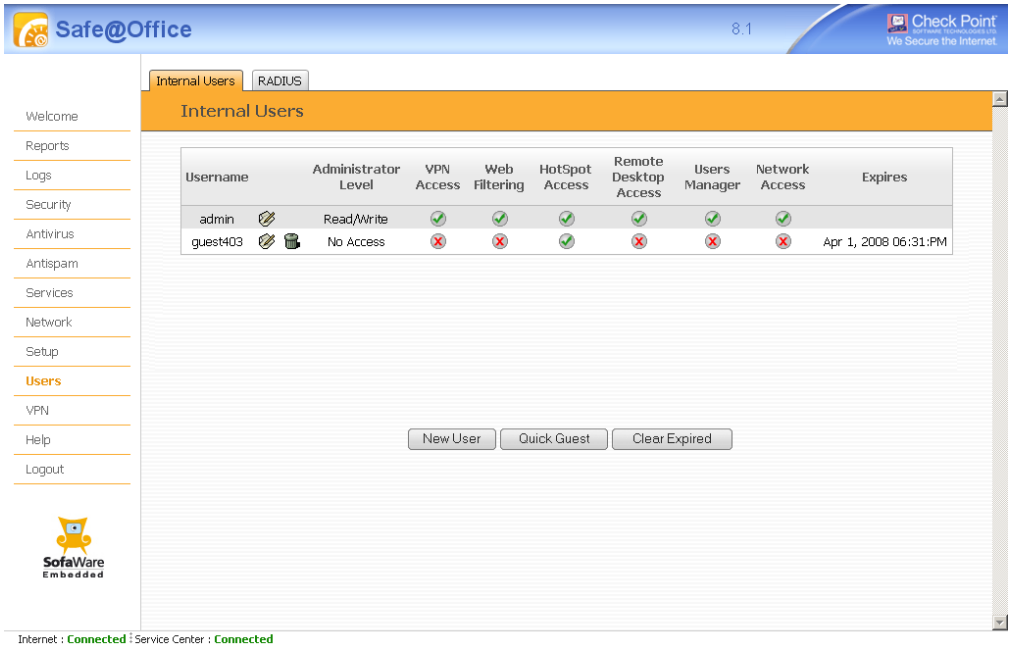
500 1000N

You can change your username and password at any time.

To change your login credentials

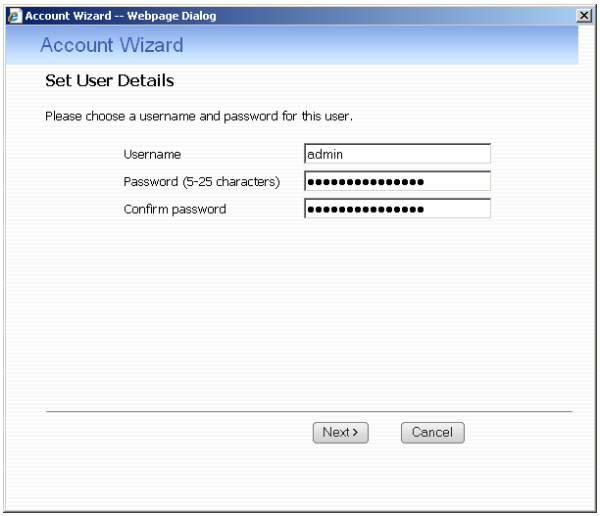
1. Click Users in the main menu, and click the Internal Users tab.

The Internal Users page appears.



2. In the row of your username, click Edit.

The **Account Wizard** opens displaying the **Set User Details** dialog box.

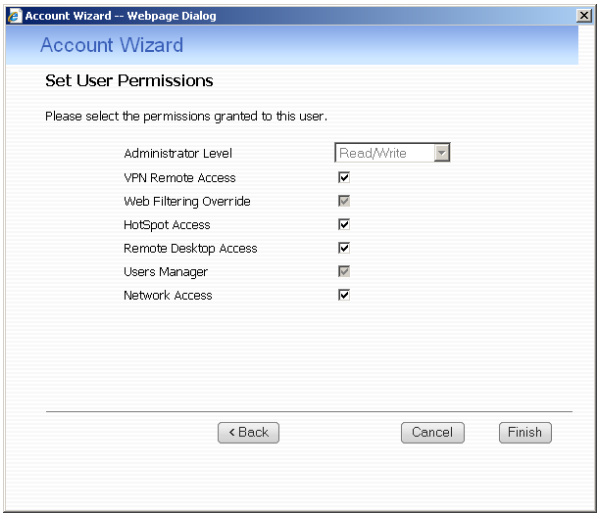


3. Edit the **Username** field.
4. Edit the **Password** and **Confirm password** fields.

Note: Use 5 to 25 characters (letters or numbers) for the new password.

5. Click **Next**.

The Set User Permissions dialog box appears.



6. Click Finish.

   Your changes are saved.

Adding and Editing Users

500 1000N

This procedure explains how to add and edit users.

For information on quickly adding guest HotSpot users via a shortcut that the Safe@Office appliance provides, see ***Adding Quick Guest HotSpot Users*** on page 685.

To add or edit a user

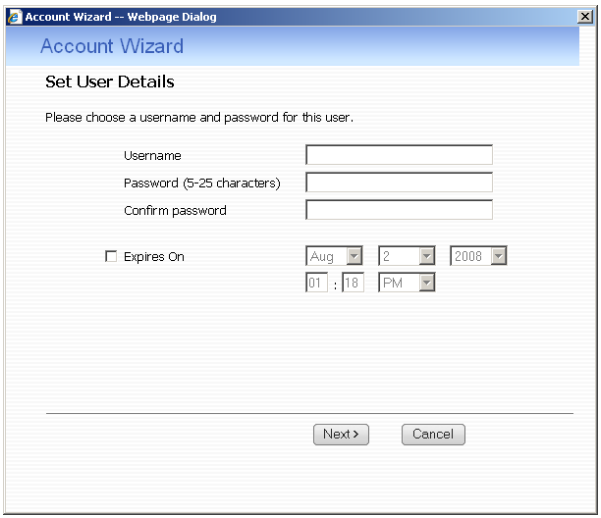
1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.

2. Do one of the following:

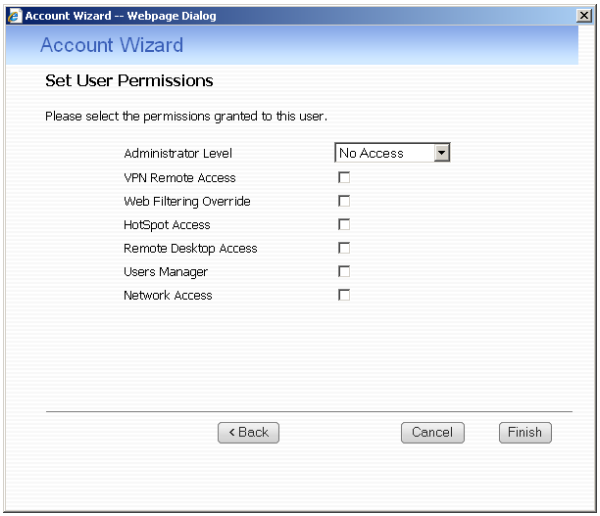
   - To create a new user, click New User.
   - To edit an existing user, click next to the desired user.

The Account Wizard opens displaying the Set User Details dialog box.



3. Complete the fields using the information in ***Set User Details Fields*** on page 682.
4. Click Next.

   The Set User Permissions dialog box appears.



The options that appear on the page are dependant on the software and services you are using.

5. Complete the fields using the information in ***Set User Permissions Fields*** on page 683.
6. Click Finish.

   The user is saved.

Table 142: Set User Details Fields

In this field…	Do this…
Username	Enter a username for the user.
Password	Enter a password for the user. Use five to 25 characters (letters or numbers) for the new password.
Confirm Password	Re-enter the user's password.
Expires On	To specify an expiration time for the user, select this option and specify the expiration date and time in the fields provided. When the user account expires, it is locked, and the user can no longer log in to the Safe@Office appliance. If you do not select this option, the user will not expire.

Table 143: Set User Permissions Fields

In this field...	Do this...
Administrator Level	Select the user's level of access to the Safe@Office Portal. The levels are: • No Access: The user cannot access the Safe@Office Portal. • Read Only: The user can log in to the Safe@Office Portal, but cannot modify system settings or export the appliance configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. • Read/Write: The user can log in to the Safe@Office Portal and modify system settings. The default level is No Access. The "admin" user's Administrator Level (Read/Write) cannot be changed.
VPN Remote Access	Select this option to allow the user to connect to this Safe@Office appliance using their VPN client. For further information on setting up VPN remote access, see ***Setting Up Remote VPN Access for Users*** on page 687
Web Filtering Override	Select this option to allow the user to override the Web Filtering service and Web rules. This option cannot be changed for the "admin" user.
HotSpot Access	Select this option to allow the user to log in to the My HotSpot page. For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 419. This option only appears in Safe@Office <500PP>.

Remote Desktop Access	Select this option to allow the user to log in to the my.firewall portal, view the My Computers page, and remotely access computers' desktops, using the Remote Desktop feature. Note: The user can perform these actions, even if their level of administrative access is "No Access". For information on Remote Desktop, see ***Using Remote Desktop*** on page 699.
Users Manager	Select this option to allow the user to log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users, but not modify other system settings. For example, you could assign this administrator level to clerks who need to manage HotSpot users.
Network Access	Select this option to allow the user to connect to this Safe@Office appliance via a wireless client or by connecting to the appliance's ports, when the Safe@Office EAP authenticator is used. For information on the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 433.

Adding Quick Guest HotSpot Users

500 1000N

The Safe@Office appliance provides a shortcut for quickly adding a guest HotSpot user. This is useful in situations where you want to grant temporary network access to guests, for example in an Internet café. The shortcut also enables printing the guest user's details in one click.

By default, the quick guest user has the following characteristics:

- Username in the format `guest<number>`, where `<number>` is a unique three-digit number.

  For example: guest123
- Randomly generated password
- Expires in 24 hours
- Administration Level: No Access
- Permissions: HotSpot Access only

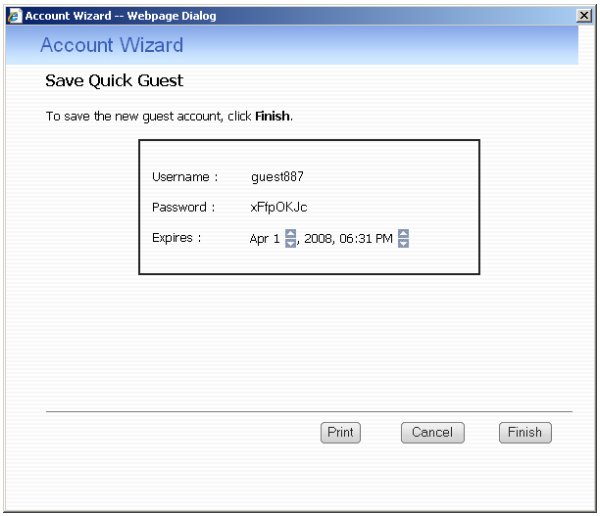
For information on configuring Secure HotSpot, see ***Using Secure HotSpot*** on page 419. For information on changing the default expiration period, refer to the *Embedded NGX CLI Reference Guide*.

To quickly create a guest user

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.
2. Click Quick Guest.

The Account Wizard opens displaying the Save Quick Guest dialog box.



3. In the Expires field, click on the arrows to specify the expiration date and time.
4. To print the user details, click Print.
5. Click Finish.

   The guest user is saved.

   You can edit the guest user's details and permissions using the procedure ***Adding and Editing Users*** on page 680.

Viewing and Deleting Users

500 1000N

To view or delete users

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears with a list of all users and their permissions.

   The expiration time of expired users appears in red.
2. To delete a user, do the following:

a) In the desired user's row, click .
   A confirmation message appears.
b) Click OK.
   The user is deleted.

3. To delete all expired users, do the following:
   a) Click Clear Expired.
      A confirmation message appears.
   b) Click OK.
      The expired users are deleted.

Setting Up Remote VPN Access for Users

500 1000N

If you are using your Safe@Office appliance as a SecuRemote Remote Access VPN Server, as an internal VPN Server, or as an L2TP VPN Server, you can allow users to access it remotely through their Remote Access VPN Clients (a Check Point SecureClient, Check Point SecuRemote, an L2TP VPN Client, an Endpoint Connect client, or another Embedded NGX appliance).

To set up remote VPN access for a user

1. Enable your VPN Server, using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 607.
2. Add or edit the user, using the procedure ***Adding and Editing Users*** on page 680.

   You must select the VPN Remote Access option.

Using RADIUS Authentication

500 1000N

You can use Remote Authentication Dial-In User Service (RADIUS) to authenticate both Safe@Office appliance users and Remote Access VPN Clients trying to connect to the Safe@Office appliance.

Note: When RADIUS authentication is in use, the Safe@Office appliance must have a certificate.

When a user tries to log in to the Safe@Office Portal, the Safe@Office appliance sends the entered user name and password to the RADIUS server. The server then checks whether the RADIUS database contains a matching user name and password pair. If so, then the user is logged in.

By default, all RADIUS-authenticated users are assigned the set of permissions specified in the Safe@Office Portal's RADIUS page. However, you can configure the RADIUS server to pass the Safe@Office appliance a specific set of permissions to grant the authenticated user, instead of these default permissions. This is done by configuring the RADIUS Vendor-Specific Attribute (VSA) with a set of attributes containing permission information for specific users. If the VSA is configured for a user, then the RADIUS server passes the VSA to the Safe@Office appliance as part of the response to the authentication request, and the gateway assigns the user permissions as specified in the VSA. If the VSA is not returned by the RADIUS server for a specific user, the gateway will use the default permission set for this user.

In addition, you can configure the RADIUS server to pass the Safe@Office appliance a Secure HotSpot session timeout value. When the RADIUS server's Session-Timeout Attribute is configured, HotSpot users will be logged out after the specified session timeout has elapsed.

Finally, you can track network usage, by configuring RADIUS accounting. When this option is enabled, the Safe@Office appliance sends session information to the RADIUS server at the begining and end of a user session, including the unique session identifier, session start/end time, and additional statistical data. This data can then be used to charge the user for network usage and to compile performance reports. For example, when Secure HotSpot is enabled, you can use RADIUS accounting to measure HotSpot sessions and bill HotSpot users accordingly. You can also use third-party products with the RADIUS server

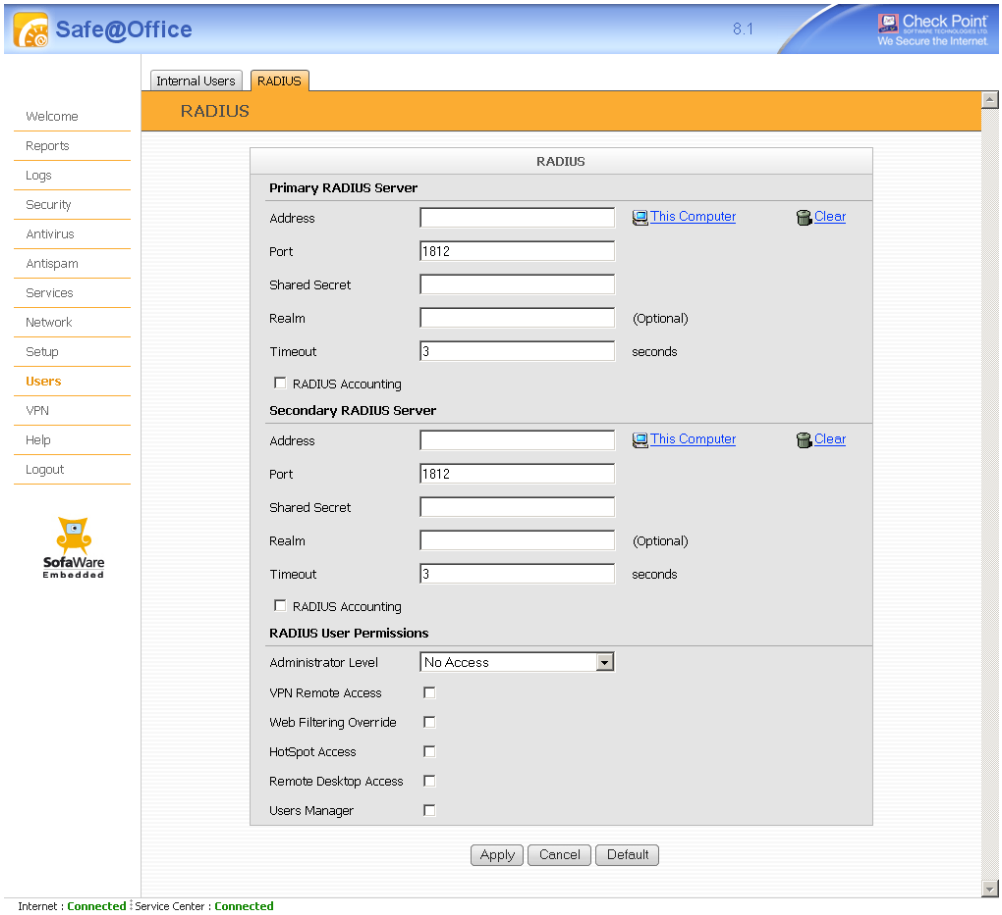
to analyze RADIUS accounting data and generate performance reports for Secure HotSpot usage.

Note: You can configure the Safe@Office appliance to send accounting information to the RADIUS server throughout the entire session. This allows for richer data collection. For information, refer to the Embedded NGX CLI Reference Guide.

To use RADIUS authentication

1. Click Users in the main menu, and click the RADIUS tab.

   The RADIUS page appears.



2. Complete the fields using the following table.
3. Click Apply.
4. To restore the default RADIUS settings, do the following:
   a) Click Default.
      A confirmation message appears.
   b) Click OK.
      The RADIUS settings are reset to their defaults. For information on the default values, refer to the following table.
5. If desired, configure user permissions and/or the HotSpot session timeout on the RADIUS server.

   See ***Configuring RADIUS Attributes*** on page 694.

Table 144: RADIUS Page Fields

In this field…	Do this…
Primary/Secondary RADIUS Server	Configure the primary and secondary RADIUS servers. By default, the Safe@Office appliance sends a request to the primary RADIUS server first. If the primary RADIUS server does not respond after three attempts, the Safe@Office appliance will send the request to the secondary RADIUS server.
Address	Type the IP address of the computer that will run the RADIUS service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service. To clear the text box, click Clear.
Port	Type the port number on the RADIUS server's host computer. The default port number is 1812.
Shared Secret	Type the shared secret to use for secure communication with the RADIUS server.

In this field...	Do this...
Realm	If your organization uses RADIUS realms, type the realm to append to RADIUS requests. The realm will be appended to the username as follows: <username>@<realm> For example, if you set the realm to “myrealm”, and the user "JohnS" attempts to log in to the Safe@Office Portal, the Safe@Office appliance will send the RADIUS server an authentication request with the username “JohnS@myrealm”. This field is optional.
Timeout	Type the interval of time in seconds between attempts to communicate with the RADIUS server. The default value is 3 seconds.
RADIUS Accounting	Select this option to enabling RADIUS accounting on the server. The Accounting Port field and the Advanced Accounting area appear.
Accounting Port	Type the port number on the RADIUS server's host computer to use for RADIUS accounting purposes. The default port number is 1813.
RADIUS User Permissions	If the RADIUS VSA (Vendor-Specific Attribute) is configured for a user, the fields in this area will have no effect, and the user will be granted the permissions specified in the VSA. If the VSA is not configured for the user, the permissions configured in this area will be used.

In this field...	Do this...
Administrator Level	Select the level of access to the Safe@Office Portal to assign to all users authenticated by the RADIUS server. The levels are: • No Access: The user cannot access the Safe@Office Portal. • Read Only: The user can log in to the Safe@Office Portal, but cannot modify system settings or export the appliance configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. • Read/Write: The user can log in to the Safe@Office Portal and modify system settings. The default level is No Access.
VPN Remote Access	Select this option to allow all users authenticated by the RADIUS server to connect to this Safe@Office appliance using their VPN client. For further information on setting up VPN remote access, see ***Setting Up Remote VPN Access for Users*** on page 687.
Web Filtering Override	Select this option to allow all users authenticated by the RADIUS server to override Web Filtering. This option only appears if the Web Filtering service is defined.
HotSpot Access	Select this option to allow all users authenticated by the RADIUS server to access the My HotSpot page. For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 419. This option only appears in Safe@Office <500PP>.

In this field...	Do this...
Remote Desktop Access	Select this option to allow all users authenticated by the RADIUS server to log in to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops, using the Remote Desktop feature. Note: Authenticated users can perform these actions, even if their level of administrative access is "No Access". For information on Remote Desktop, see ***Using Remote Desktop*** on page 699.
Users Manager	Select this option to allow all users authenticated by the RADIUS server to log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users, but not modify other system settings. For example, you could assign this administrator level to clerks who need to manage HotSpot users.
Advanced Accounting	If you enabled RADIUS accounting, this area appears.
Send Periodic Updates	Select this option to specify that the Safe@Office appliance should send accounting information to the RADIUS server throughout a user session. If you do not select this option, the Safe@Office appliance will only send accounting information to the RADIUS server at the beginning and end of the session.
Update Interval	The interval of time in seconds, at which the Safe@Office appliance should send accounting information to the RADIUS server during a session. The default value is 0.

Configuring RADIUS Attributes

500 1000N

To configure a timeout for Secure HotSpot sessions

- Set the Session-Timeout Attribute (attribute 27) to the number of seconds after which users should be automatically logged out from the hotspot.

To assign permissions to specific RADIUS-authenticated users

1. Create a remote access policy as follows:
   a) Assign the policy's VSA (attribute 26) the SofaWare vendor code (6983).
   b) For each permission you want to grant, configure the relevant attribute of the VSA with the desired value, as described in the following table.

   For example, to assign the user VPN access permissions, set attribute number 2 to "true".
2. Assign the policy to the desired user or user group.

For detailed instructions and examples, refer to the "Configuring the RADIUS Vendor-Specific Attribute" white paper.

Table 145: VSA Syntax

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
Admin	Indicates the administrator's level of access to the Safe@Office Portal	1	String	none. The user cannot access the Safe@Office Portal. readonly. The user can log in to the Safe@Office Portal, but cannot modify system settings. users-manager. The user can log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users. However, the user cannot modify other system settings. readwrite. The user can log in to the Safe@Office Portal and modify system settings.	

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
VPN	Indicates whether the user can access the network from a Remote Access VPN Client.	2	String	**true**. The user can remotely access the network via VPN. **false**. The user cannot remotely access the network via VPN.	This permission is only relevant if the Safe@Office Remote Access VPN Server is enabled. The gateway must have a certificate.
Hotspot	Indicates whether the user can log in via the My HotSpot page.	3	String	**true**. The user can access the Internet via My HotSpot. **false**. The user cannot access the Internet via My HotSpot.	This permission is only relevant if the Secure HotSpot feature is enabled.
UFP	Indicates whether the user can override Web Filtering.	4	String	**true**. The user can override Web Filtering. **false**. The user cannot override Web Filtering.	This permission is only relevant if the Web Filtering service is enabled.

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
RemoteDesktop	Indicates whether the user can remotely access computers' desktops, using the Remote Desktop feature.	5	String	**true**. The user can log in to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops (irrespective of their level of administrative access). **false**. The user cannot remotely access computers' desktops.	This permission is only relevant if the Remote Desktop feature is enabled.

Chapter 21

Using Remote Desktop

This chapter describes how to remotely access the desktop of each of your computers, using the Safe@Office appliance's Remote Desktop feature.

This chapter includes the following topics:

Overview 699
Workflow.....700
Configuring Remote Desktop 701
Configuring the Host Computer 704
Accessing a Remote Computer's Desktop 707

Overview

500 1000N

Your Safe@Office appliance includes an integrated client for Microsoft Terminal Services, allowing you to remotely access the desktop of each of your computers from anywhere, via the Safe@Office Portal. You can even redirect your printers or ports to a remote computer, so that you can print and transfer files with ease.

Remote Desktop sessions use the Microsoft Remote Desktop Protocol (RDP) on TCP port 3389. This port is opened dynamically between the Remote Desktop client and the Remote Desktop server as needed, meaning that the port is not exposed to the Internet, and your constant security is ensured.

Note: By default, the Microsoft RDP protocol is secured with 128-bit RC4 encryption. For the strongest possible security, it is recommended to use Remote Desktop over an IPSec VPN connection. For information on VPNs, see ***Working With VPNs*** on page *601*.

Workflow

500 1000N

To use Remote Desktop

1. Configure Remote Desktop.

   See ***Configuring Remote Desktop*** on page 701.

2. Enable the Remote Desktop server on computers that authorized users should be allowed to remotely access.

   See ***Configuring the Host Computer*** on page 704.

3. Grant Remote Desktop Access permissions to users who should be allowed to remotely access desktops.

   See ***Adding and Editing Users*** on page 680.

4. The authorized users can access remote computers' desktops as desired.

   See ***Accessing a Remote Computer's Desktop*** on page 707.

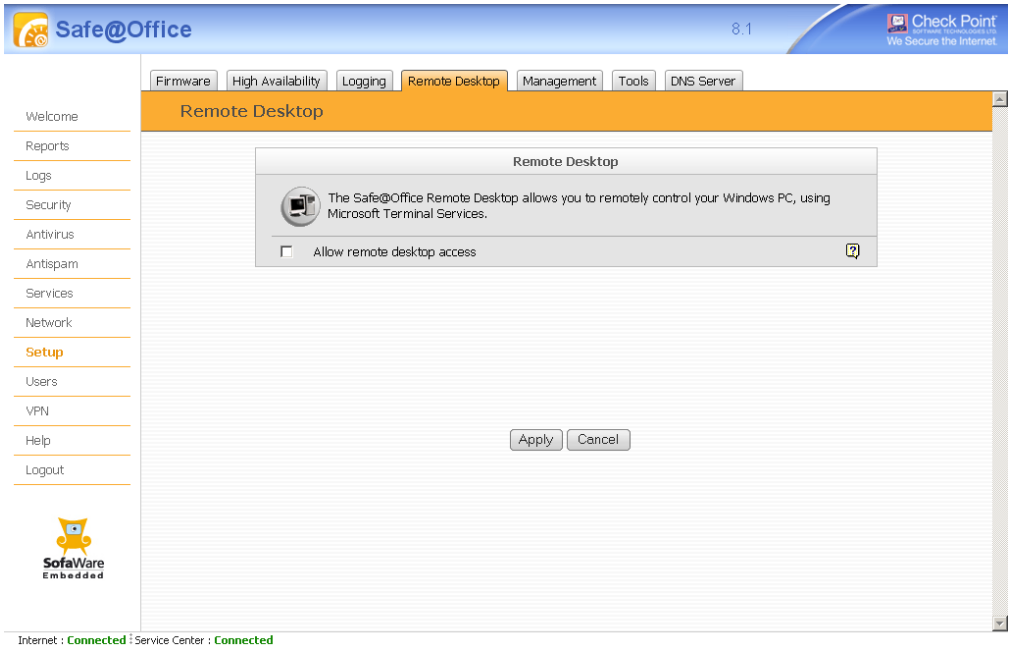
Configuring Remote Desktop

500 | 1000N

To configure Remote Desktop

1. Click Setup in the main menu, and click the Remote Desktop tab.

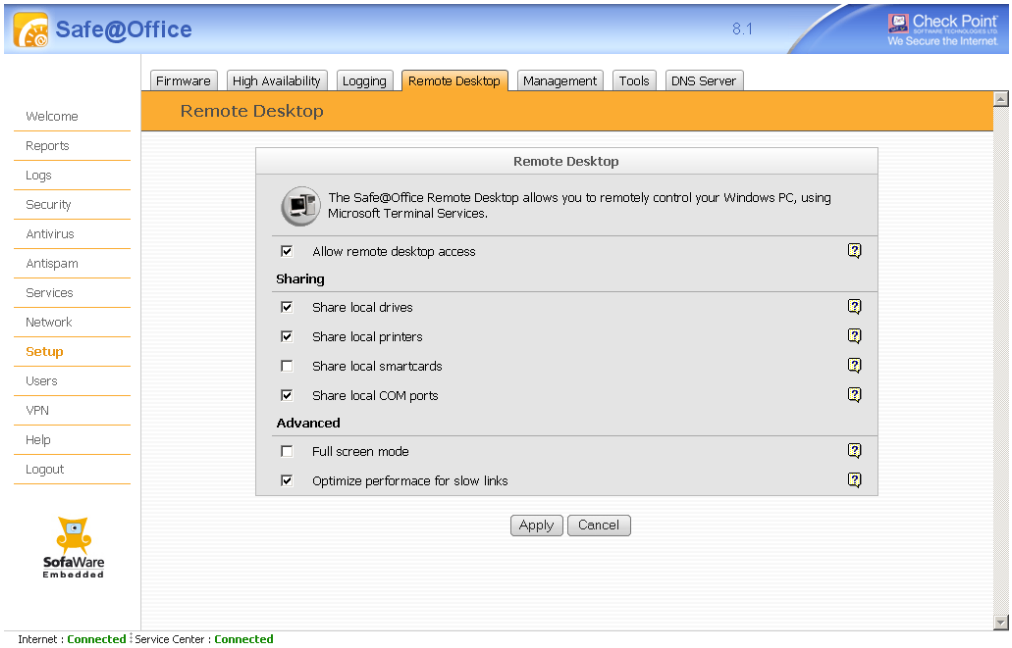
   The Remote Desktop page appears.



2. Do one of the following:

   - To enable Remote Desktop, select the Allow remote desktop access check box.

New fields appear.



- To disable Remote Desktop, clear the **Allow remote desktop access** check box. Fields disappear.

3. Complete the fields using the information in the following table.
4. Click **Apply**.

Table 146: Remote Desktop Options

In this field…	Do this…
Sharing	
Share local drives	Select this option to allow the host computer to access hard drives on the client computer. This enables remote users to access their local hard drives when logged in to the host computer.
Share local printers	Select this option to allow the host computer to access printers on the client computer. This enables remote users to access their local printer when logged in to the host computer.
Share local smartcards	Select this option to allow the host computer to access smartcards on the client computer. This enables remote users to access their local smartcards when logged in to the host computer.
Share local COM ports	Select this option to allow the host computer to access COM ports on the client computer. This enables remote users to access their local COM ports when logged in to the host computer.
Advanced	
Full screen mode	Select this option to open Remote Desktop sessions on the whole screen.
Optimize performance for slow links	Select this option to optimize Remote Desktop sessions for slow links. Bandwidth-consuming options, such as wallpaper and menu animations, will be disabled.

Configuring the Host Computer

To enable remote users to connect to a computer, you must enable the Remote Desktop server on that computer.

Note: The host computer must have one of the following operating systems installed:

- Microsoft Windows Server 2003
- Microsoft Windows XP Professional
- Microsoft Windows XP Media Center
- Microsoft Windows XP Tablet PC 2005

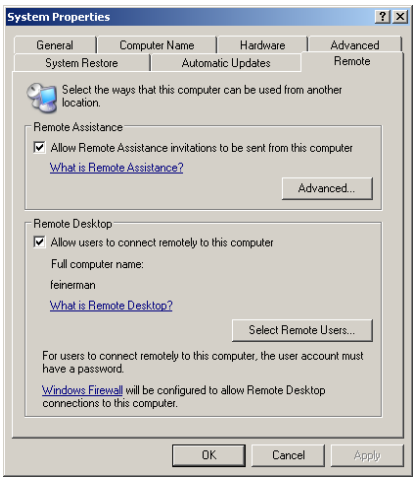
To enable users to remotely connect to a computer

1. Log on to the desired computer as an administrator.
2. For each remote user who should be allowed to access this computer, create a user account with a password.

   For information, refer to Microsoft documentation.
3. On the desktop, right-click on My Computer, and select Properties in the pop-up menu that appears.

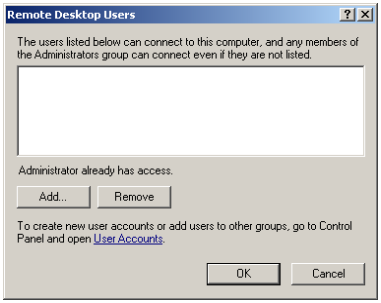
   The System Properties dialog box appears displaying the General tab.
4. Click the Remote tab.

The Remote tab appears.



5. Select the Allow users to connect remotely to this computer check box.
6. Click Select Remote Users.

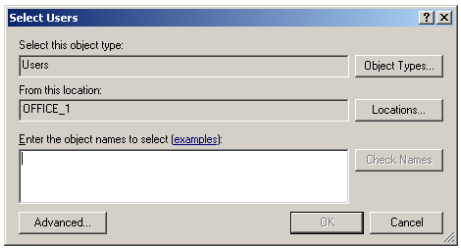
   The Remote Desktop Users dialog box appears.


Remote Desktop Users
The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.
Administrator already has access.
Add...
Remove
To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.
OK
Cancel

7. Do the following for each remote user who should be allowed to access this computer:

   a. Click Add.

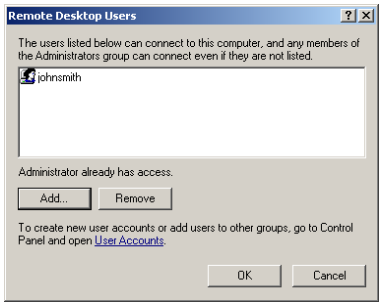
The Select Users dialog box appears.



b. Type the desired user's username in the text box.
The Check Names button is enabled.

c. Click Check Names.

d. Click OK.
The Remote Desktop Users dialog box reappears with the desired user's username.


Remote Desktop Users
The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.
johnsmith
Administrator already has access.
Add...
Remove
To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.
OK
Cancel

8. Click OK.
9. Click OK.

Accessing a Remote Computer's Desktop

500 1000N

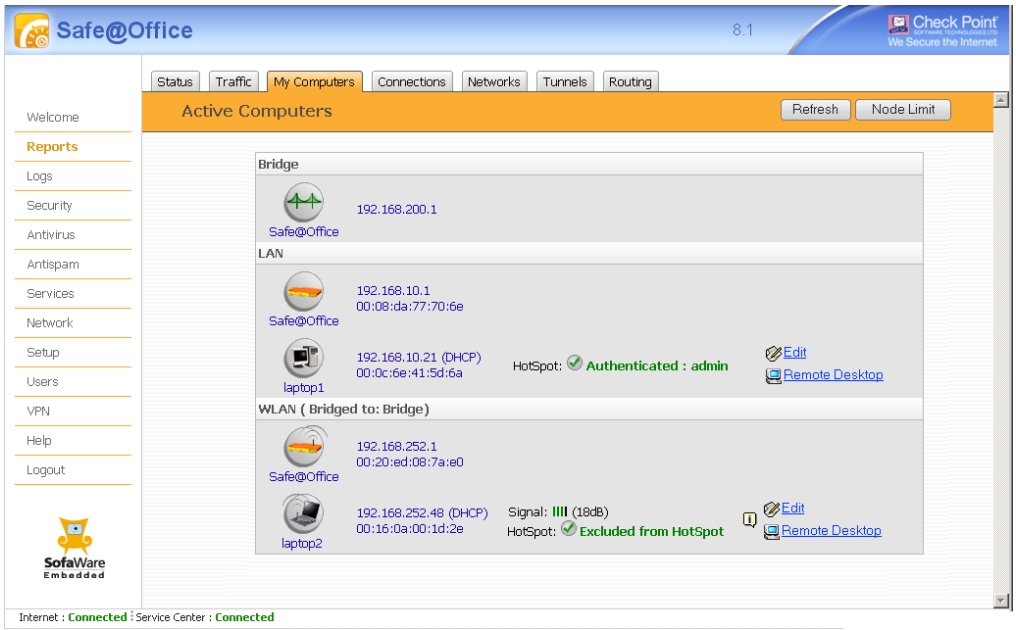
Note: The client computer must meet the following requirements:

- Microsoft Internet Explorer 6.0 or later
- A working Internet connection

To access a remote computer's desktop

1. Click Reports in the main menu, and click the My Computers tab.

   The My Computers page appears.



2. Next to the desired computer, click Remote Desktop.

   The following things happen:

   - If you are prompted to install the Remote Desktop Active X Control, then install it.

- The Remote Desktop Connection Security Warning dialog box appears.

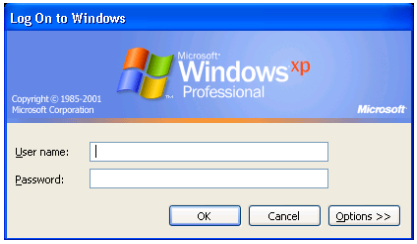
Remote Desktop Connection Security Warning
The Remote Desktop has requested a connection to your computer. Do you want to:
Connect your local disk drives to the remote computer
Connect your local ports to the remote computer
For security reasons, you may not want to allow this.
OK
Cancel

3. Select the desired connection options.

   The available options depend on your Remote Desktop configuration. See ***Configuring Remote Desktop*** on page 701.

4. Click OK.

   The Log On to Windows dialog box appears.



5. Type your username and password for the remote computer.

   These are the credentials configured for your user account in ***Enabling the Remote Desktop Server*** on page 704.

6. Click OK.

   The remote computer's desktop appears onscreen.

You can use the following keyboard shortcuts during the Remote Desktop session:

Table 147: Remote Desktop Keyboard Shortcuts

This shortcut…	Does this…
ALT+INSERT	Cycles through running programs in the order that they were started
ALT+HOME	Displays the Start menu
CTRL+ALT+BREAK	Toggles between displaying the session in a window and on the full screen
CTRL+ALT+END	Opens the Windows Security dialog box

Chapter 22

Controlling the Appliance via the Command Line

This chapter describes various ways of controlling your Safe@Office appliance through the command line.

This chapter includes the following topics:

Overview 711
Using the Safe@Office Portal 712
Using the Serial Console 714
Configuring SSH 717

Overview

500 1000N

Depending on your Safe@Office model, you can control your appliance via the command line in the following ways:

- Using the Safe@Office Portal's command line interface.

  See ***Using the Safe@Office Portal*** on page 712.

- Using a console connected to the Safe@Office appliance.

  For information, see ***Using the Serial Console*** on page 714.

- Using an SSH client.

  See ***Configuring SSH*** on page 717.

Using the Safe@Office Portal

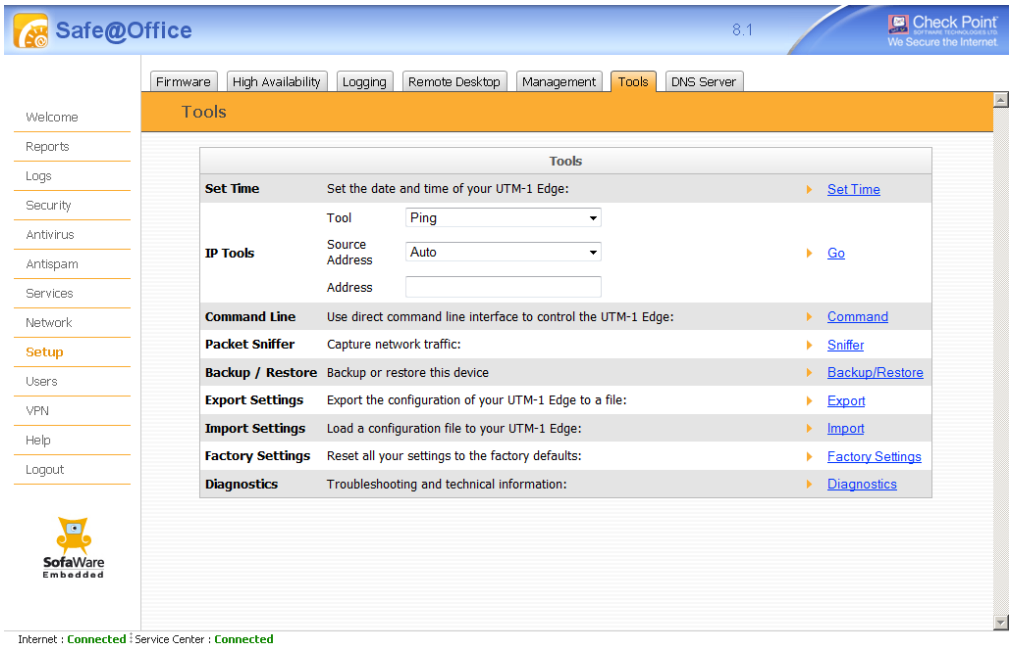
500 1000N

You can control your appliance via the Safe@Office Portal's command line interface.

To control the appliance via the Safe@Office Portal

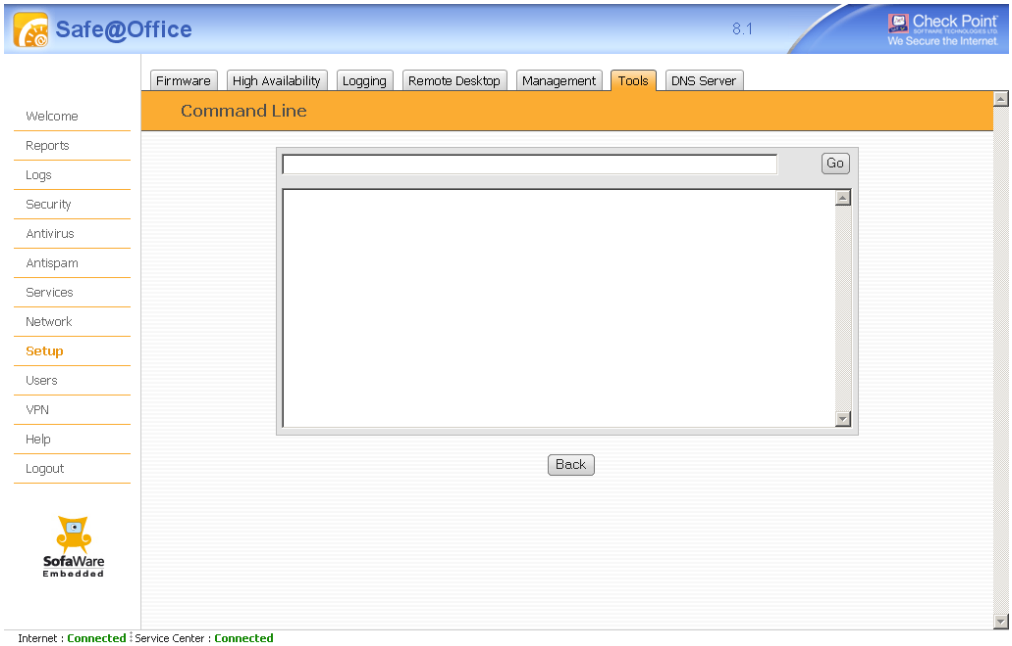
1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.



2. Click Command.

The Command Line page appears.



3. In the upper field, type a command.

   You can view a list of supported commands using the command help.

   For information on all commands, refer to the *Embedded NGX CLI Reference Guide*.

4. Click Go.

   The command is implemented.

Using the Serial Console

500 1000N

You can connect a console to the Safe@Office appliance, and use the console to control the appliance via the command line.

Note: Your terminal emulation software and your Safe@Office appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, refer to the *Embedded NGX CLI Reference Guide*.

To control the appliance via a console

1. Connect the serial console to your Safe@Office appliance's Serial port, using an RS-232 Null modem cable.

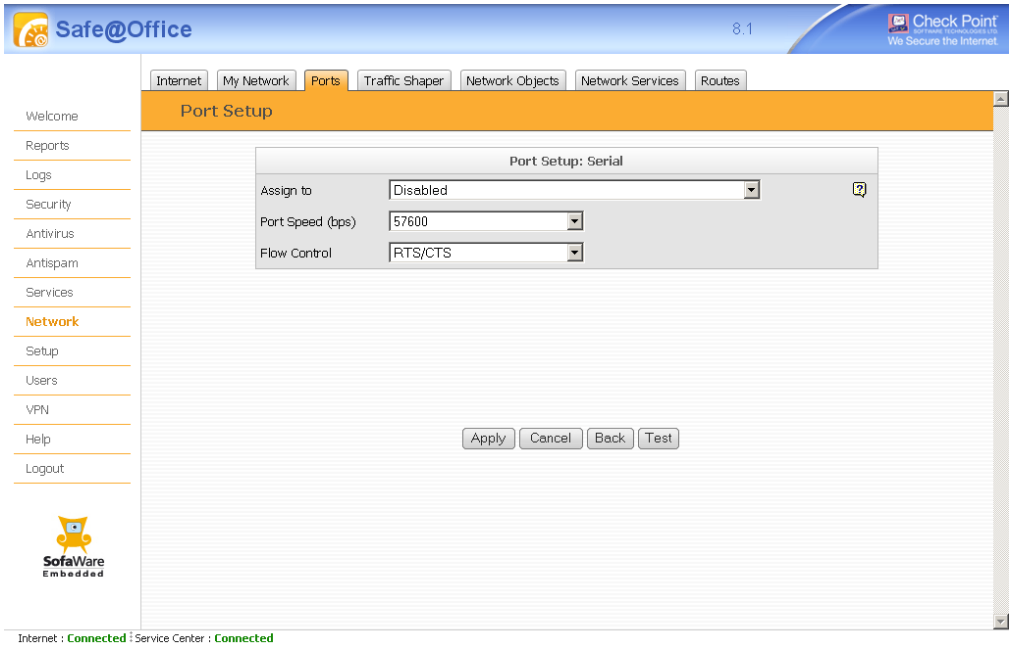
   For information on locating the Serial port, see Rear Panel.

2. Click Network in the main menu, and click the Ports tab.

The Ports page appears.

3. Next to the Serial port, click Edit.

The Port Setup page appears.



4. In the Assign to drop-down list, select Console.
5. In the Port Speed drop-down list, select the Serial port's speed (in bits per second).

   The Serial port's speed must match that of the attached serial console. The default value is 57600.
6. In the Flow Control drop-down list, select the method of flow control supported by the attached device:
   - RTS/CTS. Hardware-based flow control, using the Serial port's RTS/CTS lines.
   - XON/XOFF. Software-based flow control, using XON/XOFF characters.
7. Click Apply.

   You can now control the Safe@Office appliance from the serial console.

   For information on all supported commands, refer to the *Embedded NGX CLI Reference Guide*.

Configuring SSH

500 1000N

Safe@Office appliance users can control the appliance via the command line, using the SSH (Secure Shell) management protocol. You can enable users to do so via the Internet, by configuring remote SSH access. You can also integrate the Safe@Office appliance with SSH-based management systems.

Note: The Safe@Office appliance supports SSHv2 clients only. The SSHv1 protocol contains security vulnerabilities and is not supported.

Note: Configuring SSH is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for SSH, such as allowing SSH connections from multiple IP address ranges, define Allow rules for TCP port 22, with the destination This Gateway. For information, see ***Using Rules*** on page *400*.

To configure SSH

1. Click Setup in the main menu, and click the Management tab.

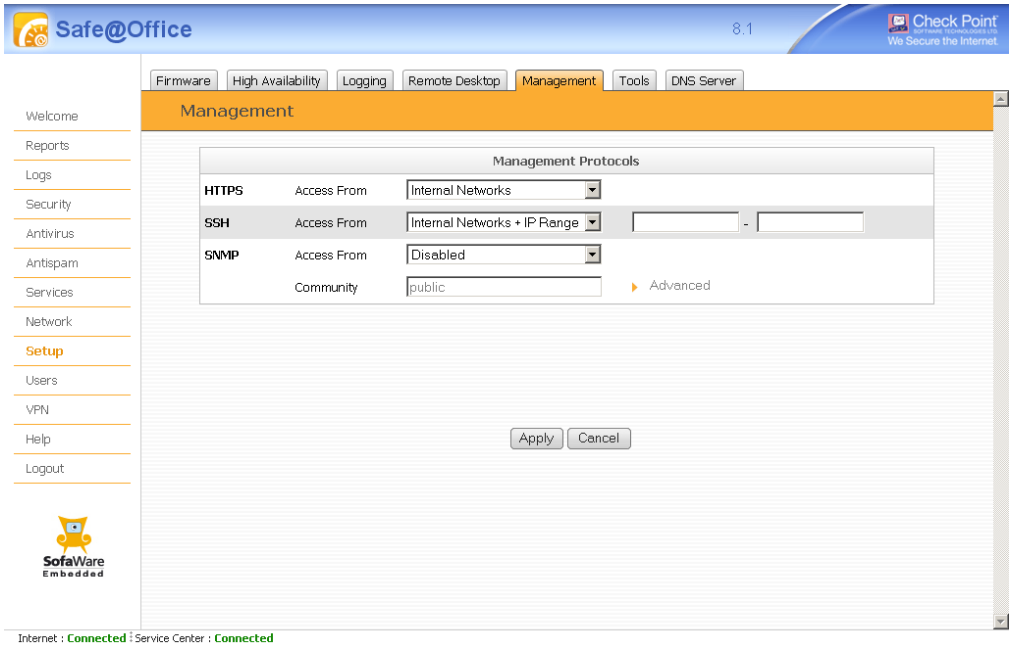
   The Management page appears.

2. Specify from where SSH access should be granted.

   Refer to the following table.

Warning: If remote SSH is enabled, your Safe@Office appliance settings can be changed remotely, so it is especially important to make sure all Safe@Office appliance users' passwords are difficult to guess.

If you selected Internal Networks + IP Range, additional fields appear.



3. If you selected Internal Networks + IP Range, enter the desired IP address range in the fields provided.
4. Click Apply.

   The SSH configuration is saved. If you configured remote SSH access, you can now control the Safe@Office appliance from the Internet, using an SSHv2 client.

   For information on all supported commands, refer to the *Embedded NGX CLI Reference Guide*.

Table 148: SSH Access Options

Select this option…	To allow access from…
Internal Networks	The internal network only. This disables remote access capability. This is the default.
Internal Networks + VPN	The internal network and your VPN.
Internal Networks + IP Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.
Disabled	Nowhere. This disables both local and remote access capability. This option is relevant to the SNMP protocol only.

Chapter 23

Maintenance

This chapter describes the tasks required for maintenance and diagnosis of your Safe@Office appliance.

This chapter includes the following topics:

Viewing Firmware Status 720
Upgrading Your Software Product 722
Configuring a Gateway Hostname....724
Configuring Syslog Logging 726
Configuring HTTPS 728
Configuring SNMP....730
Setting the Time on the Appliance 735
Using Diagnostic Tools 738
Backing Up and Restoring the Safe@Office Appliance Configuration ...752
Using Rapid Deployment 759
Resetting the Safe@Office Appliance to Defaults 762
Running Diagnostics 765
Rebooting the Safe@Office Appliance 766

Viewing Firmware Status

500 1000N

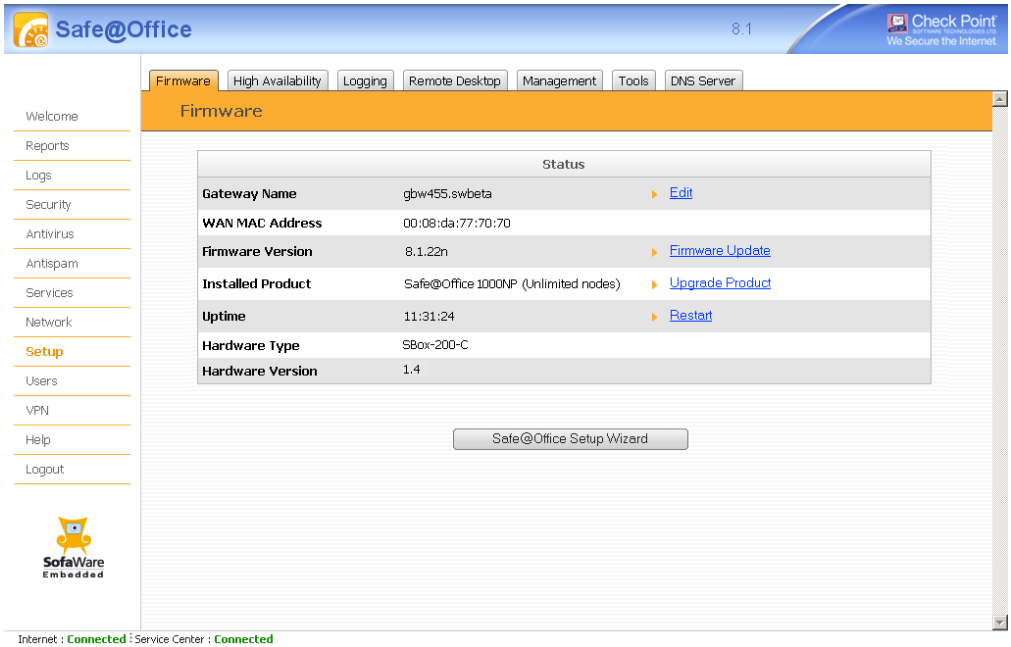
The firmware is the software program embedded in the Safe@Office appliance.

You can view your current firmware version and additional details.

To view the firmware status

- Click Setup in the main menu, and click the Firmware tab.

The Firmware page appears.



The Firmware page displays the following information:

Table 149: Firmware Status Fields

This field...	Displays...	For example...
WAN MAC Address	The MAC address used for the Internet connection	00:80:11:22:33:44
Firmware Version	The current version of the firmware	8.1
Installed Product	The licensed software and the number of allowed nodes	Safe@Office 1000N (unlimited nodes)

This field…	Displays…	For example…
Uptime	The time that elapsed from the moment the unit was turned on	01:21:15
Hardware Type	The type of the current Safe@Office appliance hardware	SBox-200
Hardware Version	The current hardware version of the Safe@Office appliance	

Upgrading Your Software Product

500 1000N

You can upgrade your Safe@Office 1000N appliance by adding the Safe@Office 1000N Power Pack. After purchasing the Power Pack, you will receive a new Product Key that enables you to use the Power Pack on the same Safe@Office appliance you have today. There is no need to replace your hardware. You can also purchase node upgrades, as needed.

Note: To purchase the Power Pack or node upgrades, contact your Safe@Office appliance provider. Alternatively, you can click Upgrades & Services in the Welcome page to view and purchase available upgrades.

To upgrade your product, you must install the new Product Key.

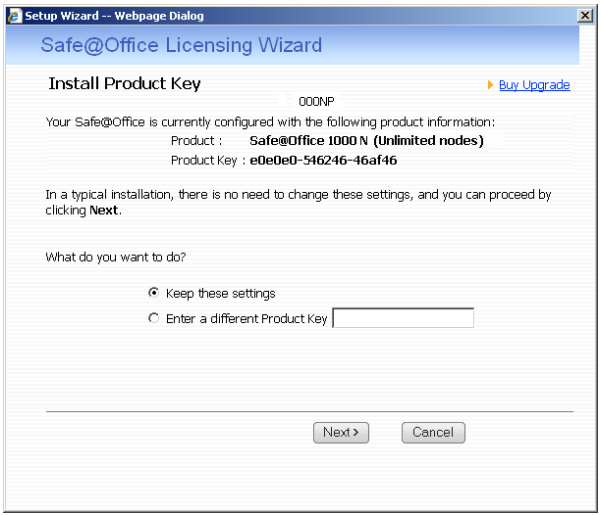
To install a Product Key

1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.

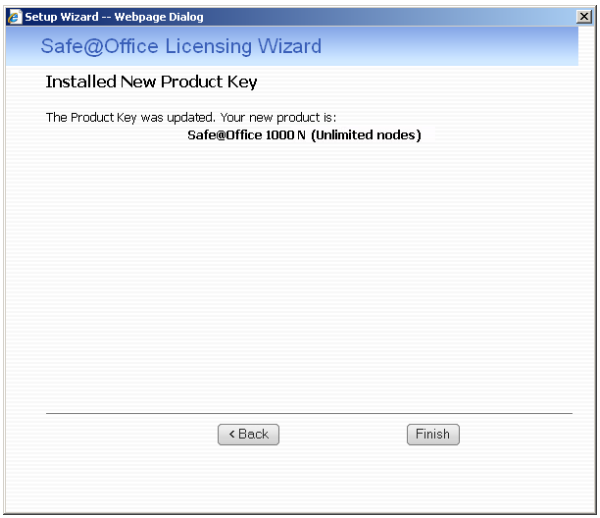
2. Click Upgrade Product.

The Safe@Office Licensing Wizard opens, with the Install Product Key dialog box displayed.


Setup Wizard -- Webpage Dialog
Safe@Office Licensing Wizard
Install Product Key
Buy Upgrade
000NP
Your Safe@Office is currently configured with the following product information:
Product : Safe@Office 1000 N (Unlimited nodes)
Product Key : e0e0e0-546246-46af46
In a typical installation, there is no need to change these settings, and you can proceed by clicking Next.
What do you want to do?
Keep these settings
Enter a different Product Key
Next >
Cancel

3. Click Enter a different Product Key.
4. In the Product Key field, enter the new Product Key.
5. Click Next.

   The Installed New Product Key dialog box appears.


Setup Wizard -- Webpage Dialog
Safe@Office Licensing Wizard
Installed New Product Key
The Product Key was updated. Your new product is:
Safe@Office 1000 N (Unlimited nodes)
< Back
Finish

6. Click Finish.

Configuring a Gateway Hostname

500 1000N

You can define a gateway hostname for the Safe@Office appliance. The gateway hostname is used to identify the Safe@Office appliance and appears in the following places:

- The Safe@Office Portal's title bar
- The Safe@Office appliance's SNMP hostname
- Syslog messages sent by the Safe@Office appliance
- The command line prompt

By default, the Safe@Office appliance's MAC address is used as the gateway hostname.

Note: Configuring the gateway hostname is only available if the Safe@Office appliance is not subscribed to the Remote Management service. When remotely managed, the gateway hostname is set by the Service Center.

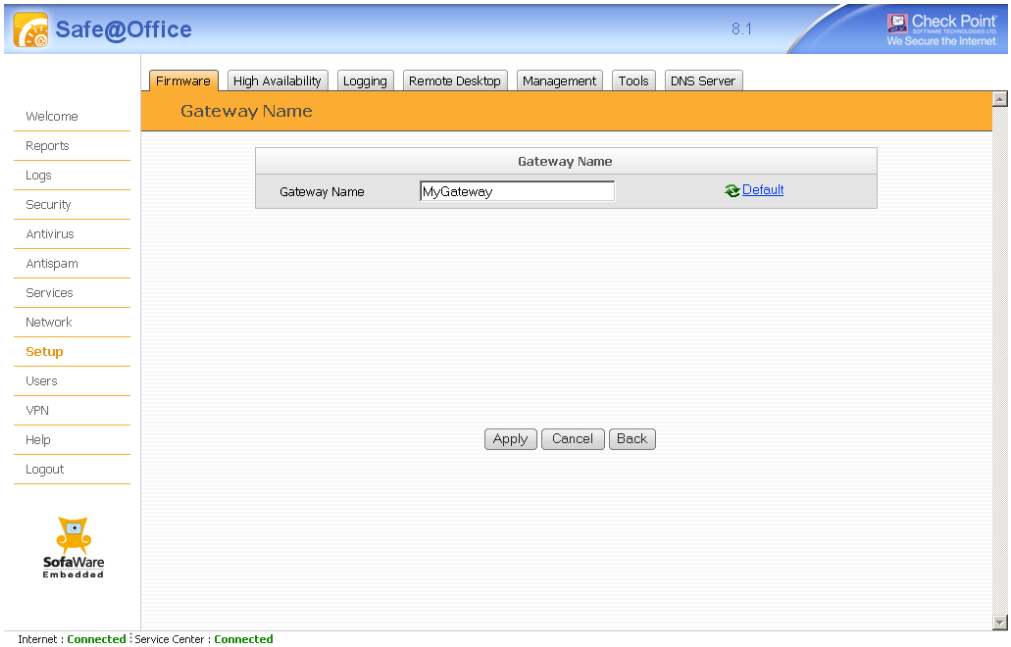
To configure the gateway hostname

1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.

2. In the Gateway Name row, click Edit.

The Gateway Name page appears.



3. In the Gateway Name field, type the desired hostname.
4. To reset the gateway hostname to the default value (the appliance's MAC address), click Default.
5. Click Apply.

Configuring Syslog Logging

500 1000N

You can configure the Safe@Office appliance to send event logs to a Syslog server residing in your internal network or on the Internet. The logs detail the date and the time each event occurred. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

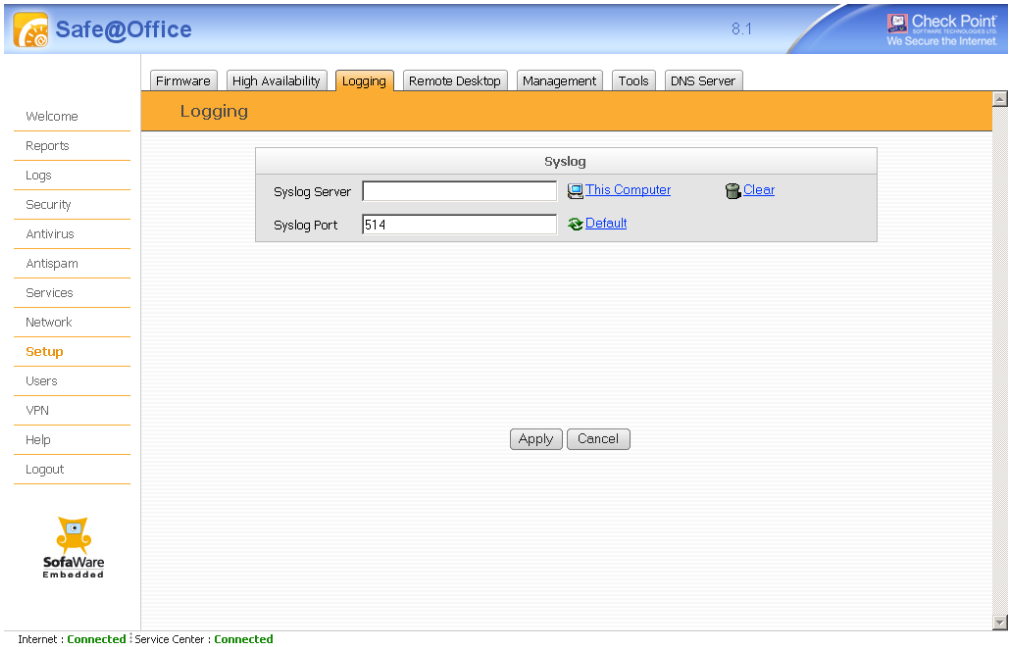
This same information is also available in the Event Log page (see ***Viewing the Event Log*** on page 379). However, while the Event Log can display hundreds of logs, a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

Note: Kiwi Syslog Daemon is freeware and can be downloaded from http://www.kiwisyslog.com. For technical support, contact Kiwi Enterprises.

To configure Syslog logging

1. Click Setup in the main menu, and click the Logging tab.

The Logging page appears.



2. Complete the fields using the information in the following table.
3. Click Apply.

Table 150: Logging Page Fields

In this field...	Do this...
Syslog Server	Type the IP address of the computer that will run the Syslog service (one of your network computers), or click This Computer to allow your computer to host the service.
Clear	Click to clear the Syslog Server field.
Syslog Port	Type the port number of the Syslog server.
Default	Click to reset the Syslog Port field to the default (port 514 UDP).

Configuring HTTPS

500 1000N

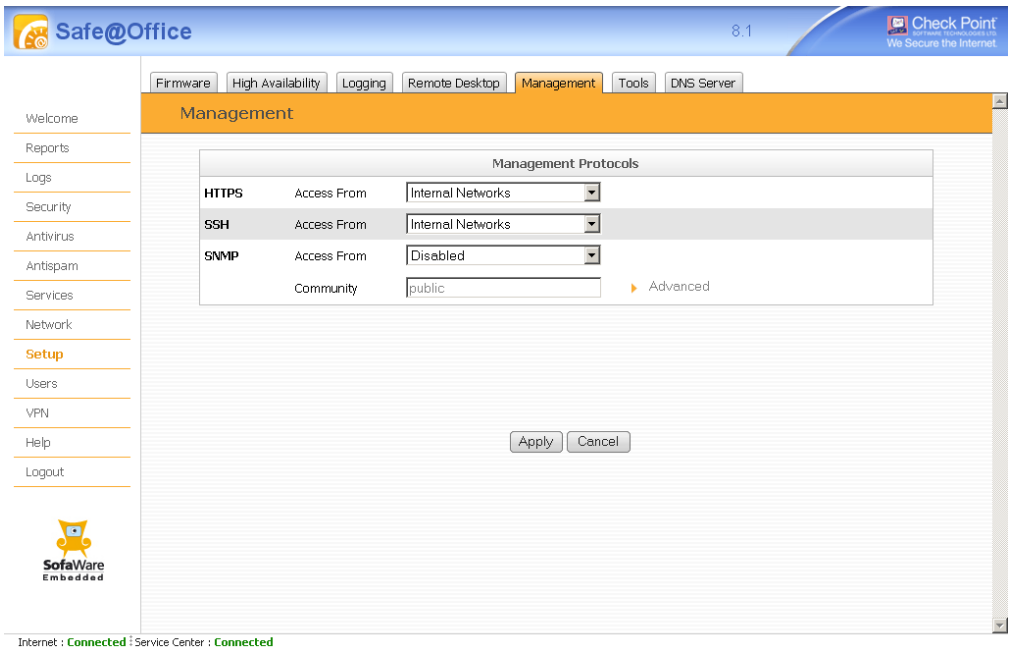
You can enable Safe@Office appliance users to access the Safe@Office Portal from the Internet. To do so, you must first configure HTTPS.

Note: Configuring HTTPS is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for HTTPS, such as allowing HTTPS connections from multiple IP address ranges, define Allow rules for TCP port 443, with the destination This Gateway. For information, see ***Using Rules*** on page *400*.

To configure HTTPS

1. Click Setup in the main menu, and click the Management tab.

   The Management page appears.



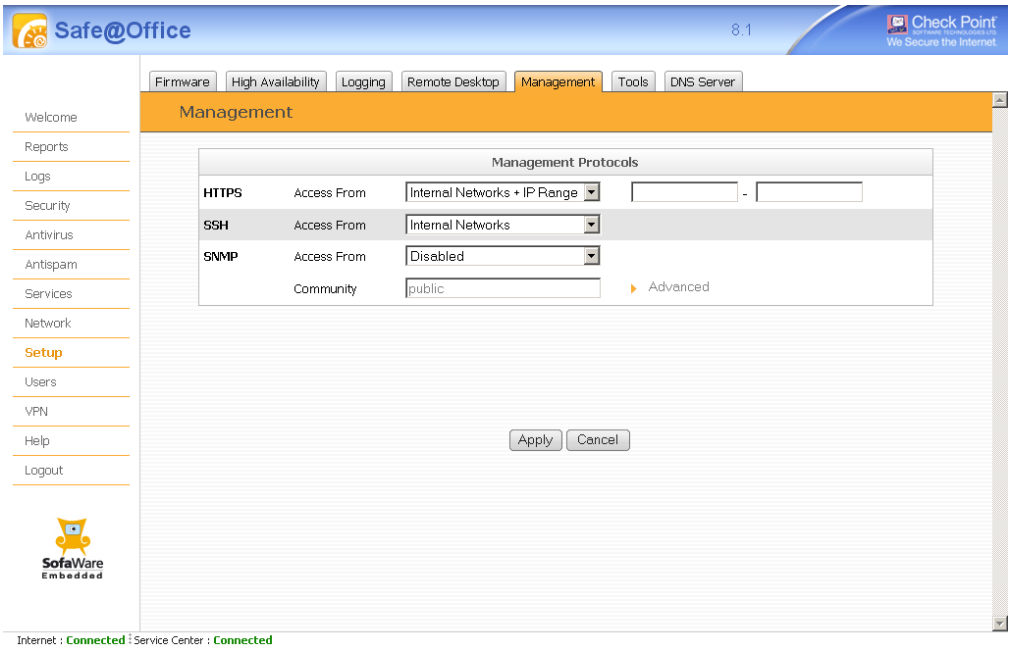
2. Specify from where HTTPS access to the Safe@Office Portal should be granted.

   See ***Access Options*** on page 730 for information.

Warning: If remote HTTPS is enabled, your Safe@Office appliance settings can be changed remotely, so it is especially important to make sure all Safe@Office appliance users' passwords are difficult to guess.

Note: You can use HTTPS to access the Safe@Office Portal from your internal network, by surfing to https://my.firewall.

If you selected Internal Networks + IP Range, additional fields appear.



3. If you selected Internal Networks + IP Range, enter the desired IP address range in the fields provided.
4. Click Apply.

   The HTTPS configuration is saved. If you configured remote HTTPS, you can now access the Safe@Office Portal through the Internet, using the procedure ***Accessing the Safe@Office Portal Remotely*** on page 116.

Table 151: Access Options

Select this option…	To allow access from…
Internal Networks	The internal network only. This disables remote access capability. This is the default.
Internal Networks + VPN	The internal network and your VPN.
Internal Networks + IP Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.
Disabled	Nowhere. This disables both local and remote access capability. This option is relevant to the SNMP protocol only.

Configuring SNMP

500 1000N

Safe@Office appliance users can monitor the Safe@Office appliance, using tools that support SNMP (Simple Network Management Protocol). You can enable users to do so via the Internet, by configuring remote SNMP access.

The Safe@Office appliance supports the following SNMP MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB

- IP-MIB

All SNMP access is read-only.

Note: Configuring SNMP is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for SNMP, such as allowing SNMP connections from multiple IP address ranges, define Allow rules for the relevant port (by default, TCP port 161), with the destination This Gateway. For information, see ***Using Rules*** on page *400*.

To configure SNMP

1. Click Setup in the main menu, and click the Management tab.

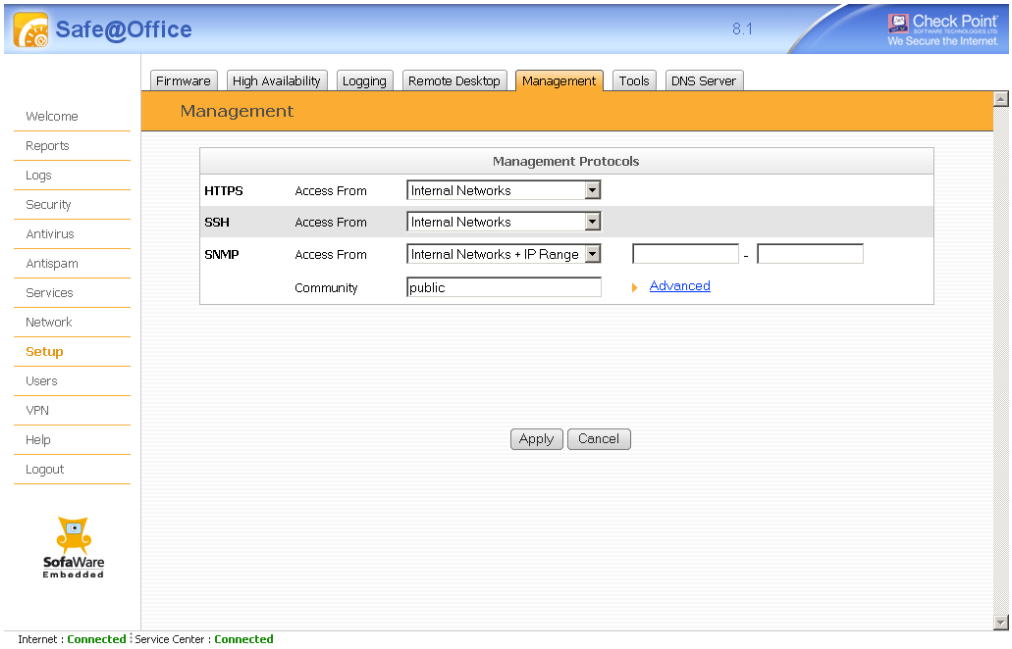
   The Management page appears.

2. Specify from where SNMP access should be granted.

   See ***Access Options*** on page 730 for information.

   If you selected Internal Networks + IP Range, additional fields appear.

   The Community field and the Advanced link are enabled.



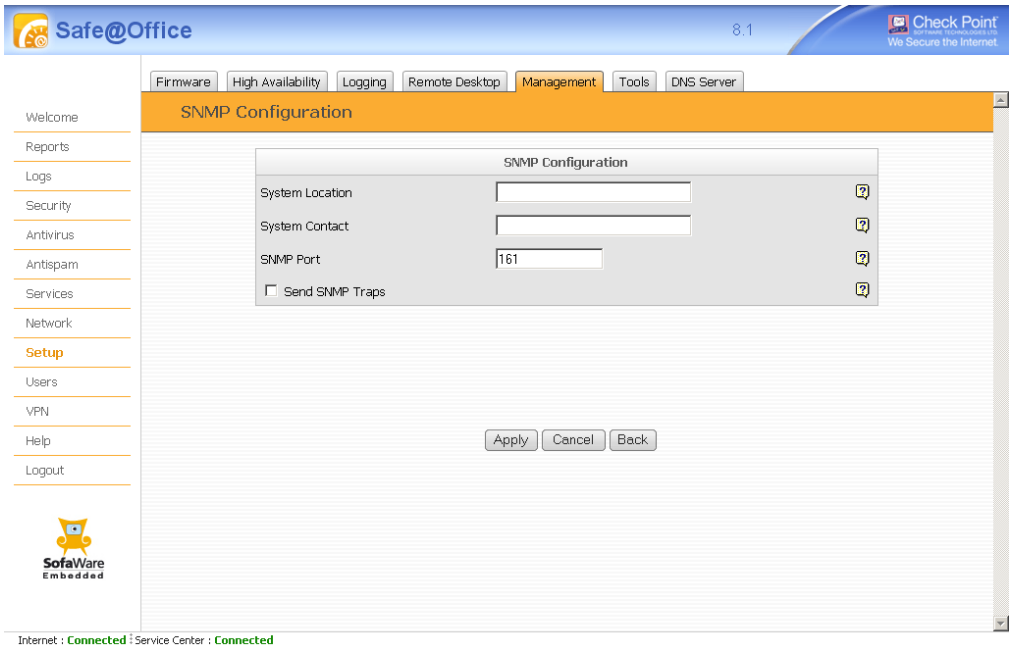
3. If you selected Internal Networks + IP Range, enter the desired IP address range in the fields provided.
4. In the Community field, type the name of the SNMP community string.

   SNMP clients uses the SNMP community string as a password, when connecting to the Safe@Office appliance.

   The default value is "public". It is recommended to change this string.
5. To configure advanced SNMP settings, do the following:

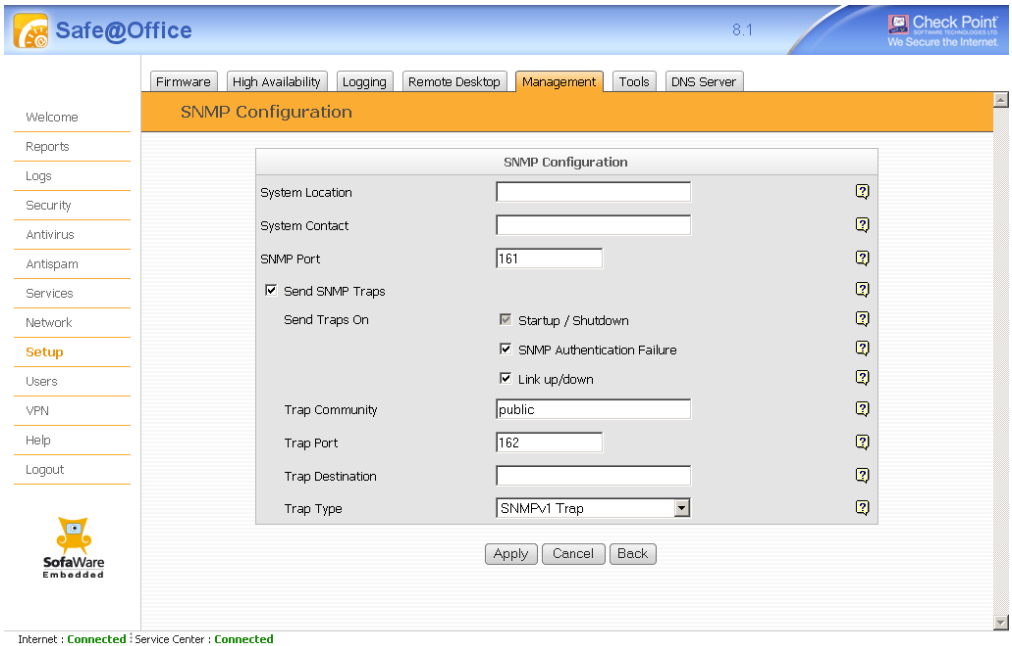
   a. Click Advanced.

   The SNMP Configuration page appears.



   b. Complete the fields using the following table.

If you selected the Send SNMP Traps check box, additional fields appear.



6. Click Apply.

   The SNMP configuration is saved.

7. Configure the SNMP clients with the SNMP community string.

Table 152: Advanced SNMP Settings

In this field...	Do this...
System Location	Type a description of the appliance's location. This information will be visible to SNMP clients, and is useful for administrative purposes.
System Contact	Type the name of the contact person. This information will be visible to SNMP clients, and is useful for administrative purposes.

In this field...	Do this...
SNMP Port	Type the port to use for SNMP. The default port is 161.
Send SNMP Traps	Select this option to enable sending SNMP traps. An SNMP trap is a notification sent from one application to another.
Send Traps On: Startup / Shutdown	Indicates that SNMP traps will automatically be sent upon startup/shutdown events. This option is always selected.
Send Traps On: SNMP Authentication Failure	Select this option to to send an SNMP trap on each SNMP authentication failure event.
Send Traps On: Link up/down	Select this option to send an SNMP trap on each link up/down event.
Trap Community	Type the SNMP community string of the trap receiver. The default value is `public`.
Trap Port	Type The UDP port of the trap receiver. The default value is 162.
Trap Destination	Type the IP address or DNS name of the SNMP trap receiver agent.
Trap Type	Select the type of SNMP traps to use.

Setting the Time on the Appliance

500 1000N

You set the time displayed in the Safe@Office Portal during initial appliance setup. If desired, you can change the date and time using the procedure below.

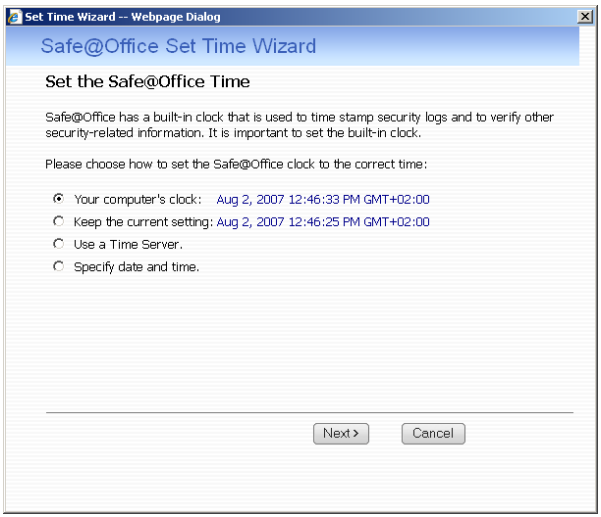
To set the time

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Set Time.

   The Safe@Office Set Time Wizard opens displaying the Set the Safe@Office Time dialog box.

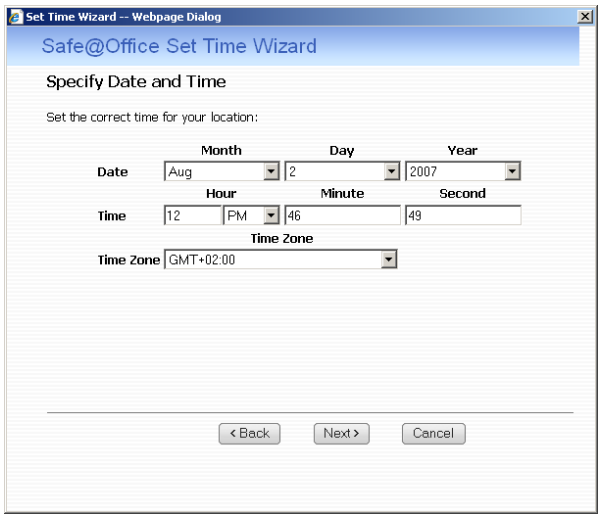

Set Time Wizard -- Webpage Dialog
Safe@Office Set Time Wizard
Set the Safe@Office Time
Safe@Office has a built-in clock that is used to time stamp security logs and to verify other security-related information. It is important to set the built-in clock.
Please choose how to set the Safe@Office clock to the correct time:
Your computer's clock: Aug 2, 2007 12:46:33 PM GMT+02:00
Keep the current setting: Aug 2, 2007 12:46:25 PM GMT+02:00
Use a Time Server.
Specify date and time.
Next >
Cancel

3. Complete the fields using the information in ***Set Time Wizard Fields*** on page 737.

4. Click Next.

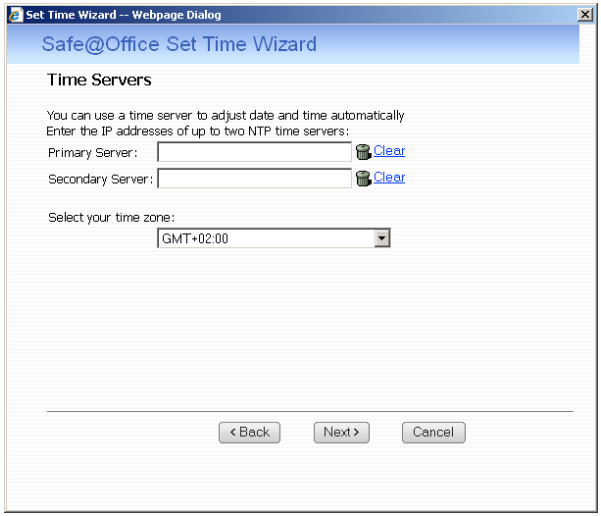
The following things happen in the order below:

- If you selected **Specify date and time**, the **Specify Date and Time** dialog box appears.



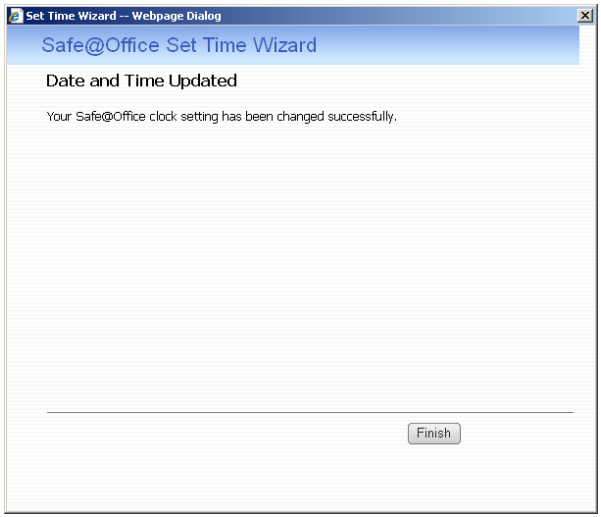
Set the date, time, and time zone in the fields provided, then click **Next**.

- If you selected **Use a Time Server**, the **Time Servers** dialog box appears.



Complete the fields using the information in ***Time Servers Fields*** on page 738, then click **Next**.

- The Date and Time Updated screen appears.


Set Time Wizard -- Webpage Dialog
Safe@Office Set Time Wizard
Date and Time Updated
Your Safe@Office clock setting has been changed successfully.
Finish

5. Click Finish.

Table 153: Set Time Wizard Fields

Select this option…	To do the following…
Your computer's clock	Set the appliance time to your computer's system time. Your computer's system time is displayed to the right of this option.
Keep the current setting	Do not change the appliance's time. The current appliance time is displayed to the right of this option.
Use a Time Server	Synchronize the appliance time with a Network Time Protocol (NTP) server.
Specify date and time	Set the appliance to a specific date and time.

Table 154: Time Servers Fields

In this field…	Do this…
Primary Server	Type the IP address of the Primary NTP server.
Secondary Server	Type the IP address of the Secondary NTP server. This field is optional.
Clear	Clear the field.
Select your time zone	Select the time zone in which you are located.

Using Diagnostic Tools

500 1000N

The Safe@Office appliance is equipped with a set of diagnostic tools that are useful for troubleshooting Internet connectivity.

Table 155: Diagnostic Tools

Use this tool…	To do this…	For information, see…
Ping	Check that a specific IP address or DNS name can be reached via the Internet.	***Using IP Tools*** on page 739
Traceroute	Display a list of all routers used to connect from the Safe@Office appliance to a specific IP address or DNS name.	***Using IP Tools*** on page 739
WHOIS	Display the name and contact information of the entity to which a specific IP address or DNS name is registered. This information is useful in tracking down hackers.	***Using IP Tools*** on page 739

Use this tool...	To do this...	For information, see...
Packet Sniffer	Capture network traffic. This information is useful troubleshooting network problems.	***Using Packet Sniffer*** on page 741

Using IP Tools

500 1000N

To use an IP tool

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

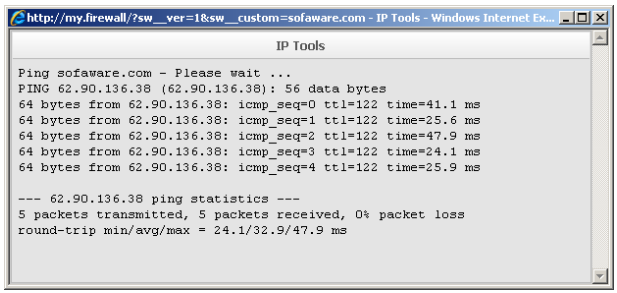
2. In the IP Tools area, complete the fields using the information in the following table.

3. Click Go.

   - If you selected Ping, the following things happen:

     The Safe@Office appliance sends packets to the specified the IP address or DNS name.

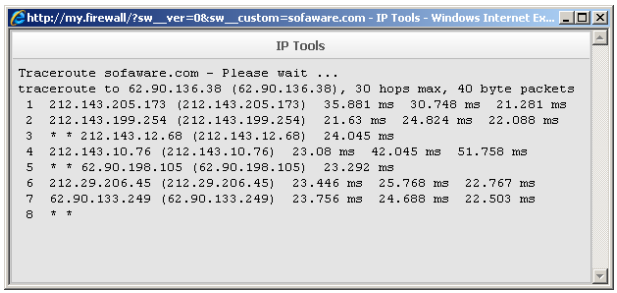
     The IP Tools window opens and displays the percentage of packet loss and the amount of time it took each packet to reach the specified host and return (round-trip) in milliseconds.


http://my.firewall/?sw__ver=1&sw__custom=sofaware.com - IP Tools - Windows Internet Ex...
IP Tools
Ping sofaware.com - Please wait ...
PING 62.90.136.38 (62.90.136.38): 56 data bytes
64 bytes from 62.90.136.38: icmp_seq=0 ttl=122 time=41.1 ms
64 bytes from 62.90.136.38: icmp_seq=1 ttl=122 time=25.6 ms
64 bytes from 62.90.136.38: icmp_seq=2 ttl=122 time=47.9 ms
64 bytes from 62.90.136.38: icmp_seq=3 ttl=122 time=24.1 ms
64 bytes from 62.90.136.38: icmp_seq=4 ttl=122 time=25.9 ms
--- 62.90.136.38 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 24.1/32.9/47.9 ms

   - If you selected Traceroute, the following things happen:

     The Safe@Office appliance connects to the specified IP address or DNS name.

The IP Tools window opens and displays a list of routers used to make the connection.



- If you selected WHOIS, the following things happen:

  The Safe@Office appliance queries the Internet WHOIS server.

  A window displays the name of the entity to which the IP address or DNS name is registered and their contact information.

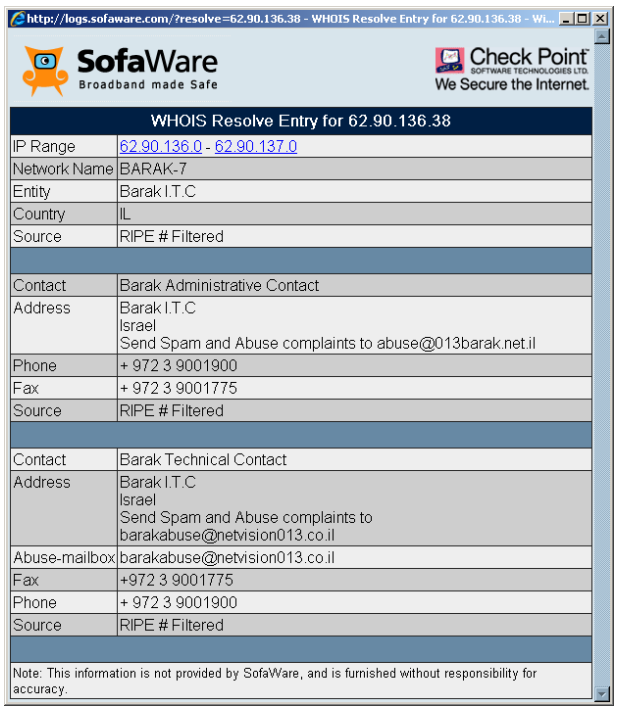

http://logs.sofaware.com/?resolve=62.90.136.38 - WHOIS Resolve Entry for 62.90.136.38 - Wi...
SofaWare
Broadband made Safe
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
WHOIS Resolve Entry for 62.90.136.38
IP Range 62.90.136.0 - 62.90.137.0
Network Name BARAK-7
Entity Barak I.T.C
Country IL
Source RIPE # Filtered
Contact Barak Administrative Contact
Address Barak I.T.C
Israel
Send Spam and Abuse complaints to abuse@013barak.net.il
Phone + 972 3 9001900
Fax + 972 3 9001775
Source RIPE # Filtered
Contact Barak Technical Contact
Address Barak I.T.C
Israel
Send Spam and Abuse complaints to
barakabuse@netvision013.co.il
Abuse-mailbox barakabuse@netvision013.co.il
Fax +972 3 9001775
Phone + 972 3 9001900
Source RIPE # Filtered
Note: This information is not provided by SofaWare, and is furnished without responsibility for accuracy.

Table 156: IP Tools Fields

In this field…	Do this…
Tool	Select the desired tool.
Source Address	Select the IP address from which the packets should originate. This can be any of the following: • Auto. Automatically select a connected or enabled interface form which to send the packets. • A connected Internet connection • An enabled internal network This field is only enabled if you selected the Ping or Traceroute tools.
Address	Type the IP address or DNS name for which to run the tool.

Using Packet Sniffer

500 1000N

The Safe@Office appliance includes the Packet Sniffer tool, which enables you to capture packets from any internal network or Safe@Office port. This is useful for troubleshooting network problems and for collecting data about network behavior.

If desired, you can configure Packet Sniffer to capture each packet twice: once before firewall processing and once after firewall processing. This allows you to observe exactly what the Safe@Office firewall does to your packets.

The Safe@Office appliance saves the captured packets to a file on your computer. You can use a free protocol analyzer, such as Ethereal or Wireshark, to analyze the file, or you can send it to technical support. Wireshark runs on all popular computing platforms and can be downloaded from http://www.wireshark.org. Ethereal can be downloaded from http://www.ethereal.com.

Note: If you enabled the Packet Sniffer's Firewall Monitor option, and you would like to view the results in Ethereal/Wireshark, you must do the following: open the capture file, click Edit > Preferences, in the left pane click Protocols > Ethernet, and select the Attempt to interpret as Firewall-1 monitor file check box. The capture file will display the interface name on which the packet was captured, and the packet's processing

direction will be indicated by i (input) or o (output).

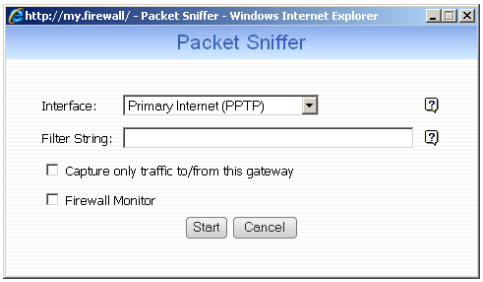
To use Packet Sniffer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Sniffer.

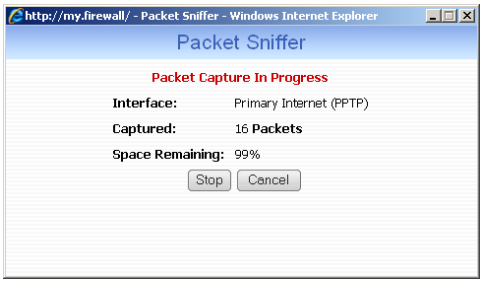
   The Packet Sniffer window opens.



3. Complete the fields using the information in the following table.

4. Click Start.

   The Packet Sniffer window displays the name of the interface, the number of packets collected, and the percentage of storage space remaining on the appliance for storing the packets.



5. Click Stop to stop collecting packets.

   A standard File Download dialog box appears.

6. Click Save.

   The Save As dialog box appears.

7. Browse to a destination directory of your choice.
8. Type a name for the configuration file and click Save.

   The *.cap file is created and saved to the specified directory.
9. Click Cancel to close the Packet Sniffer window.

Table 157: Packet Sniffer Fields

In this field…	Do this…
Interface	Select the interface from which to collect packets. The list includes the primary Internet connection, the Safe@Office appliance ports, and all defined networks.
Filter String	Type the filter string to use for filtering the captured packets. Only packets that match the filter condition will be saved. For a list of basic filter strings elements, see ***Filter String Syntax*** on page 744. For detailed information on filter syntax, go to http://www.tcpdump.org/tcpdump_man.html. Note: Do not enclose the filter string in quotation marks. If you do not specify a filter string, Packet Sniffer will save all packets on the selected interface.
Capture only traffic to/from this gateway	Select this option to capture incoming and outgoing packets for this gateway only. If this option is not selected, Packet Sniffer will collect packets for all traffic on the interface.
Firewall Monitor	Select this option to capture each packet both before and after firewall processing, and to record the name of the interface on which the packet was captured.

Filter String Syntax

The following represents a list of basic filter string elements:

- ***and*** on page 744
- ***dst*** on page 745
- ***dst port*** on page 745
- ***ether proto*** on page 746
- ***host*** on page 747
- ***not*** on page 747
- ***or*** on page 748
- ***port*** on page 748
- ***src*** on page 749
- ***src port*** on page 749
- ***tcp*** on page 750
- ***udp*** on page 751

For detailed information on filter syntax, refer to http://www.tcpdump.org.

and

PURPOSE

The `and` element is used to concatenate filter string elements. The filtered packets must match *all* concatenated filter string elements.

SYNTAX

element `and` element [`and` element...]

element && element [&& element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that both originate from IP address is 192.168.10.1 and are destined for port 80:

```
src 192.168.10.1 and dst port 80
```

dst

PURPOSE

The `dst` element captures all packets with a specific destination.

SYNTAX

dst *destination*

PARAMETERS

`destination`	IP Address or String. The computer to which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that are destined for the IP address 192.168.10.1:

```
dst 192.168.10.1
```

dst port

PURPOSE

The `dst port` element captures all packets destined for a specific port.

SYNTAX

dst port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page *750* and ***udp*** on page *751*.

PARAMETERS

`port`	Integer. The port to which the packet is sent.

EXAMPLE

The following filter string saves packets that are destined for port 80:

```
dst port 80
```

ether proto

PURPOSE

The `ether proto` element is used to capture packets of a specific ether protocol type.

SYNTAX

ether proto *protocol*

PARAMETERS

`protocol`	String. The protocol type of the packet. This can be the following: `ip`, `ip6`, `arp`, `rarp`, `atalk`, `aarp`, `dec net`, `sca`, `lat`, `mopdl`, `moprc`, `iso`, `stp`, `ipx`, or `netbeui`.

EXAMPLE

The following filter string saves ARP packets:

```
ether proto arp
```

host

PURPOSE

The `host` element captures all incoming and outgoing packets for a specific computer.

SYNTAX

host *host*

PARAMETERS

`host`	IP Address or String. The computer to/from which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves all packets that either originated from IP address 192.168.10.1, or are destined for that same IP address:

host 192.168.10.1

not

PURPOSE

The `not` element is used to negate filter string elements.

SYNTAX

not element

! element

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that are *not* destined for port 80:

```
not dst port 80
```

or

PURPOSE

The `or` element is used to alternate between string elements. The filtered packets must match at least one of the filter string elements.

SYNTAX

element or element [or element...]

element || element [|| element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that either originate from IP address 192.168.10.1 or IP address 192.168.10.10:

```
src 192.168.10.1 or src 192.168.10.10
```

port

PURPOSE

The `port` element captures all packets originating from or destined for a specific port.

SYNTAX

port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page *750* and ***udp*** on page *751*.

PARAMETERS

`port`	Integer. The port from/to which the packet is sent.

EXAMPLE

The following filter string saves all packets that either originated from port 80, or are destined for port 80:

```
port 80
```

src

PURPOSE

The `src` element captures all packets with a specific source.

SYNTAX

src *source*

PARAMETERS

`source`	IP Address or String. The computer from which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that originated from IP address 192.168.10.1:

```
src 192.168.10.1
```

src port

PURPOSE

The `src port` element captures all packets originating from a specific port.

SYNTAX

src port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page *750* and ***udp*** on page *751*.

PARAMETERS

`port`	Integer. The port from which the packet is sent.

EXAMPLE

The following filter string saves packets that originated from port 80:

```
src port 80
```

tcp

PURPOSE

The `tcp` element captures all TCP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `tcp` element is the equivalent of `ip proto tcp`.

SYNTAX

tcp

tcp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only TCP packets. This can be the following: • `dst port` - Capture all TCP packets destined for a specific port. • `port` - Capture all TCP packets originating from or destined for a specific port. • `src port` - Capture all TCP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all TCP packets:

```
tcp
```

EXAMPLE 2

The following filter string captures all TCP packets destined for port 80:

```
tcp dst port 80
```

udp

PURPOSE

The `udp` element captures all UDP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `udp` element is the equivalent of `ip proto udp`.

SYNTAX

udp

udp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only UDP packets. This can be the following: • `dst port` - Capture all UDP packets destined for a specific port. • `port` - Captures all UDP packets originating from or destined for a specific port. • `src port` - Capture all UDP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all UDP packets:

```
udp
```

EXAMPLE 2

The following filter string captures all UDP packets destined for port 80:

```
udp dst port 80
```

Backing Up and Restoring the Safe@Office Appliance Configuration

500 1000N

The Safe@Office appliance provides the following ways of backing up and restoring its configuration:

- Backup and restore on your computer

  You can export the Safe@Office appliance configuration to a *.cfg file on your computer, and use this file to backup and restore Safe@Office appliance settings, as needed.

  The file includes all of your settings, except for the security policy and certificate.

- Backup and restore on a USB flash drive

  You can back up the appliance configuration and device certificate to a USB flash drive. You can then restore the Safe@Office appliance settings from the USB flash drive as needed.

  This method requires a USB port on your appliance.

Note: In both cases, the configuration file is saved as a textual CLI script. If desired, you can edit the file. For a full explanation of the CLI script format and the supported CLI commands, see the Embedded NGX CLI Reference Guide.

Backing Up the Appliance Configuration

Exporting the Appliance Configuration to Your Computer

500 1000N

To export the Safe@Office appliance configuration to your computer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Export.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the configuration file and click Save.

   The *.cfg configuration file is created and saved to the specified directory.

   You can now import the configuration file as needed. See ***Importing the Appliance Configuration from Your Computer*** on page 756.

Backing Up the Appliance Configuration to a USB Flash Drive

USB

The USB flash drive must have at least 64MB of free space.

Note: Some USB flash drives may not be supported by the appliance.

To backup the appliance configuration to a USB flash drive

1. Connect a USB flash drive to one of your Safe@Office appliance's USB ports.

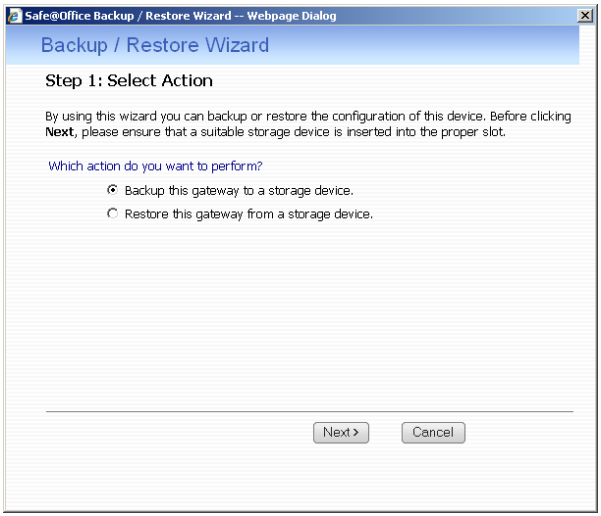
   For information on locating the USB ports, see ***Introduction*** on page 1.

2. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

3. Click Backup/Restore.

   The Backup/Restore Wizard opens displaying the Step 1: Select Action dialog box.

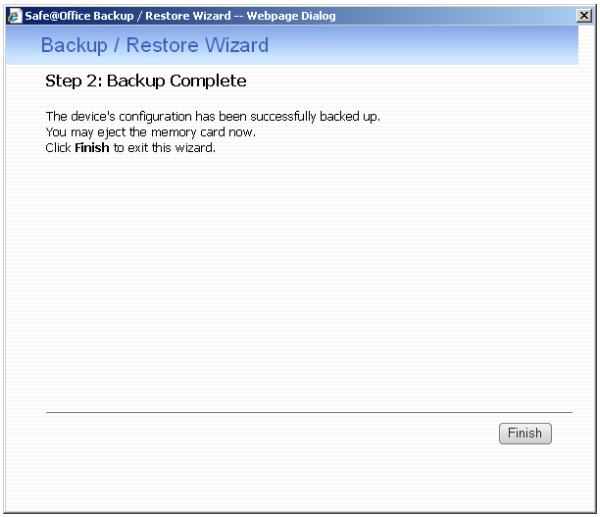

Safe@Office Backup / Restore Wizard -- Webpage Dialog
Backup / Restore Wizard
Step 1: Select Action
By using this wizard you can backup or restore the configuration of this device. Before clicking Next, please ensure that a suitable storage device is inserted into the proper slot.
Which action do you want to perform?
Backup this gateway to a storage device.
Restore this gateway from a storage device.
Next >
Cancel

4. Click Backup this gateway to a storage device.
5. Click Next.

The Safe@Office appliance creates the folder `<MACAddress>` on the USB flash drive, where `<MACAddress>` is the appliance's MAC address, and writes the following files to this folder:

- `embeddedngx.cfg`
- `embeddedngx.p12`

The Step 2: Backup Complete screen appears.


Safe@Office Backup / Restore Wizard -- Webpage Dialog
Backup / Restore Wizard
Step 2: Backup Complete
The device's configuration has been successfully backed up.
You may eject the memory card now.
Click Finish to exit this wizard.
Finish

6. Click Finish.

You can now restore the configuration from the USB flash drive as needed. See ***Restoring the Appliance Configuration from a USB Flash Drive*** on page 758.

Restoring the Appliance Configuration

Importing the Appliance Configuration from Your Computer

500 1000N

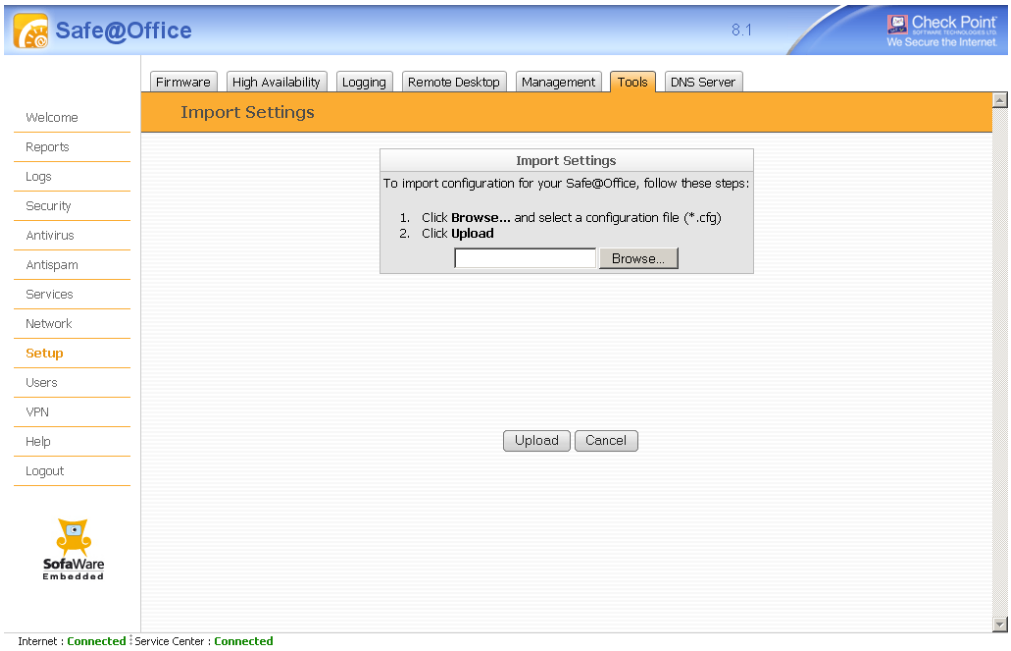
To import the appliance configuration from your computer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Import.

   The Import Settings page appears.



3. Do one of the following:

   - In the Import Settings field, type the full path to the configuration file.

   Or

   - Click Browse, and browse to the configuration file.

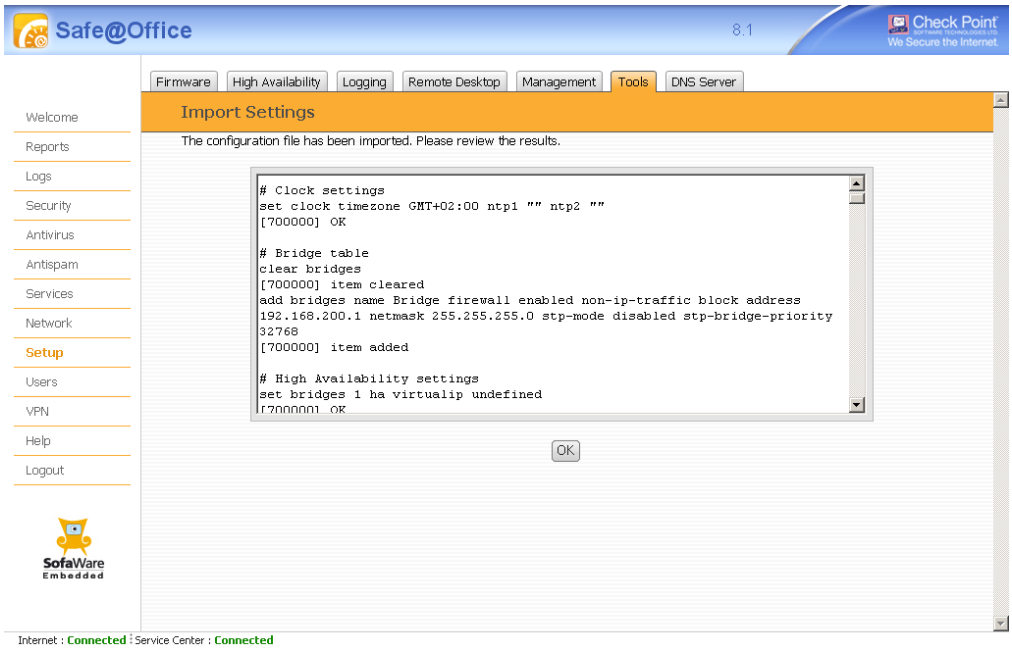
4. Click Upload.

   A confirmation message appears.

5. Click OK.

   The Safe@Office appliance settings are imported.

   The Import Settings page displays the configuration file's content and the result of implementing each configuration command.



Note: If the appliance's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

Restoring the Appliance Configuration from a USB Flash Drive

USB

To restore the appliance configuration from a USB flash drive

1. Connect a USB flash drive to one of your Safe@Office appliance's USB ports.

   For information on locating the USB ports, see ***Introduction*** on page 1.

2. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

3. Click Backup/Restore.

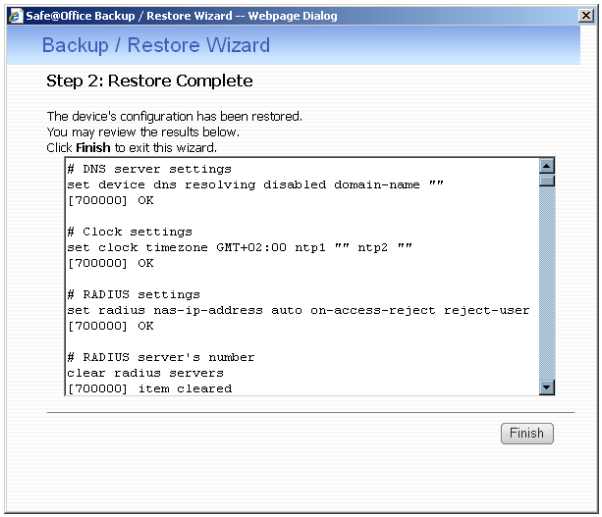
   The Backup/Restore Wizard opens displaying the Step 1: Select Action dialog box.

4. Click Restore this gateway from a storage device.

5. Click Next.

   The Safe@Office appliance is restored from the `<MACAddress>` folder on the USB flash drive, where `<MACAddress>` is the appliance's MAC address. This may take some time.

   The Step 2: Restore Complete screen appears displaying the configuration file's content and the result of implementing each configuration command.


Safe@Office Backup / Restore Wizard -- Webpage Dialog
Backup / Restore Wizard
Step 2: Restore Complete
The device's configuration has been restored.
You may review the results below.
Click Finish to exit this wizard.
DNS server settings
set device dns resolving disabled domain-name ""
[700000] OK
Clock settings
set clock timezone GMT+02:00 ntp1 "" ntp2 ""
[700000] OK
RADIUS settings
set radius nas-ip-address auto on-access-reject reject-user
[700000] OK
RADIUS server's number
clear radius servers
[700000] item cleared
Finish

Note: If the appliance's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

6. Click Finish.

Using Rapid Deployment

USB

Safe@Office appliances are shipped with a specific firmware and group of settings that represent the appliance's default state. When installing a new appliance, you can configure different settings and install new firmware versions as needed; however, this can be time-consuming. Rapid deployment avoids this hassle, by allowing you to load the following settings from a USB flash drive during product initialization:

- The primary firmware
- The backup firmware
- The configuration file
- The default configuration file

  The default configuration file contains settings that represent the desired appliance default state. The settings in the default configuration file become the appliance's new default settings and are retained even after a reset to defaults operation.

Important: The default configuration file cannot be cleared by performing a Reset to Defaults operation. It can only be cleared by loading an empty default configuration file.

- The certificate

Rapid deployment can be used to configure several appliances in succession. If multiple appliances share a group of settings, you can use rapid deployment to configure each appliance with both the shared settings and the appliance-specific settings, all in one action. For example, before shipping appliances to your company’s branch offices, you can quickly configure all of the appliances with the corporate security policy and VPN settings, as well as with branch-specific settings.

Preparing the USB Flash Drive for Rapid Deployment

USB

Before performing a rapid deployment, you must load the USB flash drive with the files you want to install on the appliance(s).

To prepare the USB flash drive

1. For each appliance you want to deploy, create a folder named `<MACAddress>`, where `<MACAddress>` is the appliance's MAC address, and the colons are replaced by underscores.

   For example, if the appliance's MAC address is 00:11:22:33:44:55, the folder name should be `00_11_22_33_44_55`.

2. If you would like to deploy multiple appliances that share settings, create a folder named `deploy`.

3. Prepare the files that you want to install on the appliances.

   The files must be named according to the following table.

4. Add files containing settings that should be shared by all of the appliances to the `deploy` folder.

5. For each appliance, add files containing settings that are specific to the appliance to the folder named after the appliance's MAC address.

For example, if you want two Safe@Office appliances to share the same primary firmware but to have different configuration files, you must prepare a single `primary.firm` file and add it to the `deploy` folder. Then you must prepare two different `embeddedngx.cfg` configuration files, and add one to each appliance's folder.

Table 158: Rapid Deployment File Names

This file...	Should be named...
The primary firmware	`primary.firm / primary.img`
The backup firmware	`secondary.firm / secondary.img`
The configuration file	`embeddedngx.cfg`
The default configuration file	`preset.cfg`
The certificate	`embeddedngx.p12`

Performing a Rapid Deployment

USB

You must perform the following procedure on each Safe@Office appliance you want to deploy.

To perform a rapid deployment

1. Reset the Safe@Office appliance to its default settings.

   See ***Resetting the Safe@Office Appliance to Defaults*** on page 762.
2. Disconnect the Safe@Office appliance from its power adapter.
3. Insert the USB flash drive into the appliance's USB port.

   For information on locating the USB ports, see ***Introduction*** on page 1.
4. Reconnect the Embedded NGX appliance to its power adapter.

   The following things happen:

   - The PWR/SEC LED flashes quickly in green, signaling that rapid deployment is in progress.
   - The file `results-<MACAddress>.log` is created in the USB flash drive's root folder, where `<MACAddress>` is the appliance's MAC address.

- If the `deploy` folder exists, the appliance loads shared settings from it. The appliance then loads its private settings from the folder named after its MAC address.

  Note: If the appliance loads an updated firmware file, the appliance restarts and then continues the rapid deployment process. Do not disconnect the USB flash drive until the process is complete.

- If an error occurs during the rapid deployment process, the PWR/SEC LED blinks quickly in red, the errors are logged to the Event Log, and rapid deployment continues.
- When rapid deployment is complete, the PWR/SEC LED is a constant green.

5. To check the results of rapid deployment, in the USB flash drive's root folder, open the file `results-<MACAddress>.log`.

   Settings that loaded successfully are marked as "ok", and settings that failed to load are marked as "failed".

Resetting the Safe@Office Appliance to Defaults

500 1000N

You can reset the Safe@Office appliance to its default settings. When you reset your Safe@Office appliance, it reverts to the state it was originally in when you purchased it.

Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your Safe@Office appliance for Internet connection. For information on performing these tasks, see ***Setting Up the Safe@Office Appliance*** on page *107*.

This operation also resets your appliance to its default Product Key. Therefore, if you upgraded your license, you should save your Product Key before resetting to defaults. You can view the installed Product Key by in the Safe@Office Licensing Wizard. For information on accessing this wizard, see ***Upgrading Your License*** on page 722.

You can reset the Safe@Office appliance to defaults via the Web management interface (software) or by manually pressing the Reset button (hardware) located at the back of the Safe@Office appliance.

When resetting the appliance via the Safe@Office Portal, you can choose to keep the current firmware or to revert to the firmware version that shipped with the Safe@Office appliance. In contrast, using the Reset button automatically reverts the firmware version.

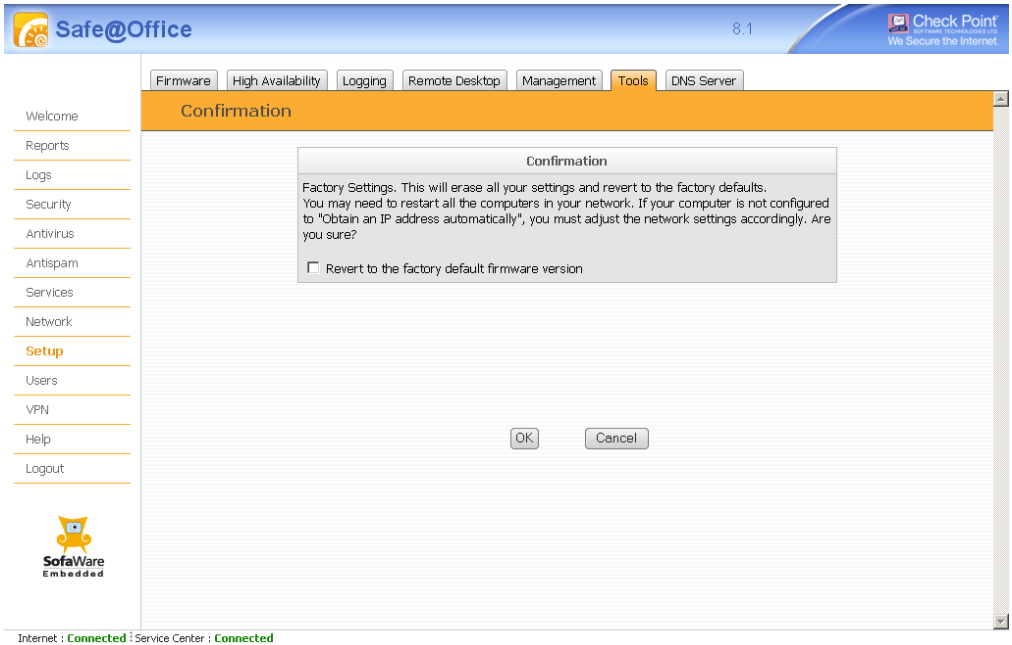
To reset the Safe@Office appliance to factory defaults via the Web interface

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Factory Settings.

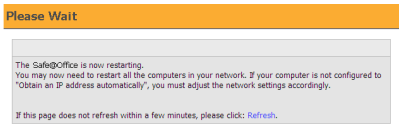
   A confirmation message appears.



3. To revert to the firmware version that shipped with the appliance, select the check box.

4. Click OK.

- The Please Wait screen appears.


Please Wait
The Safe@Office is now restarting.
You may now need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly.
If this page does not refresh within a few minutes, please click: Refresh.

- The Safe@Office appliance returns to its factory defaults.
- The Safe@Office appliance is restarted.
  This may take a few minutes.
- The Login page appears.

To reset the Safe@Office appliance to factory defaults using the Reset button

1. Make sure the Safe@Office appliance is powered on.
2. Using a pointed object, press the RESET button on the back of the Safe@Office appliance steadily for seven seconds and then release it.
3. Allow the Safe@Office appliance to boot-up until the system is ready.

   For information on the appliance's front and rear panels, see the *Getting to Know Your Appliance* section in ***Introduction*** on page 1.

Warning: If you choose to reset the Safe@Office appliance by disconnecting the power cable and then reconnecting it, be sure to leave the Safe@Office appliance disconnected for at least three seconds. Disconnecting and reconnecting the power without waiting might cause permanent damage.

Running Diagnostics

500 1000N

You can view technical information about your Safe@Office appliance's hardware, firmware, license, network status, and Service Center.

This information is useful for troubleshooting. You can export it to an *.html file and send it to technical support.

To view diagnostic information

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Diagnostics.

   Technical information about your Safe@Office appliance appears in a new window.

3. To save the displayed information to an *.html file:

   a. Click Save.
      A standard File Download dialog box appears.
   b. Click Save.
      The Save As dialog box appears.
   c. Browse to a destination directory of your choice.
   d. Type a name for the configuration file and click Save.
      The *.html file is created and saved to the specified directory.

4. To refresh the contents of the window, click Refresh.

   The contents are refreshed.

5. To close the window, click Close.

Rebooting the Safe@Office Appliance

500 1000N

If your Safe@Office appliance is not functioning properly, rebooting it may solve the problem.

To reboot the Safe@Office appliance

1. Click Setup in the main menu, and click the Firmware tab.

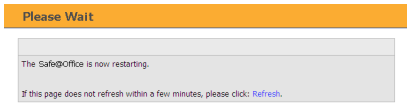
   The Firmware page appears.

2. Click Restart.

   A confirmation message appears.

3. Click OK.

   - The Please Wait screen appears.

   - The Safe@Office appliance is restarted.

     This may take a few minutes.

   - The Login page appears.

Chapter 24

Using Network Printers

This chapter describes how to set up and use network printers.

This chapter includes the following topics:

Overview 767
Setting Up Network Printers.....768
Configuring Computers to Use Network Printers.....771
Viewing Network Printers 788
Changing Network Printer Ports.....789
Resetting Network Printers.....790

Overview

Some Safe@Office models include a built-in print server, enabling you to connect USB-based printers to the appliance and share them across the network.

Note: When using computers with a Windows 2000/XP/Vista operating system, the Safe@Office appliance supports connecting up to four USB-based printers to the appliance. When using computers with a MAC OS-X operating system, the Safe@Office appliance supports connecting one printer.

The appliance automatically detects printers as they are plugged in, and they immediately become available for printing. Usually, no special configuration is required on the Safe@Office appliance.

Note: The Safe@Office print server supports printing via "all-in-one" printers. Copying and scanning functions are not supported.

Setting Up Network Printers

USB

To set up a network printer

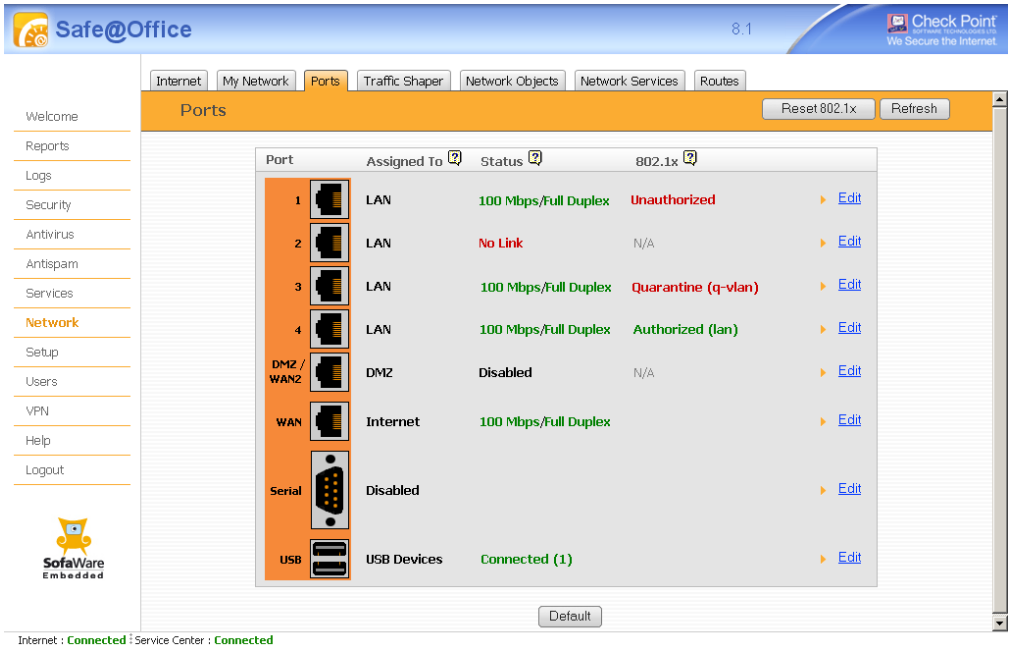
1. Connect the network printer to the Safe@Office appliance.

   See ***Connecting the Appliance to Network Printers*** on page 103.

2. Turn the printer on.

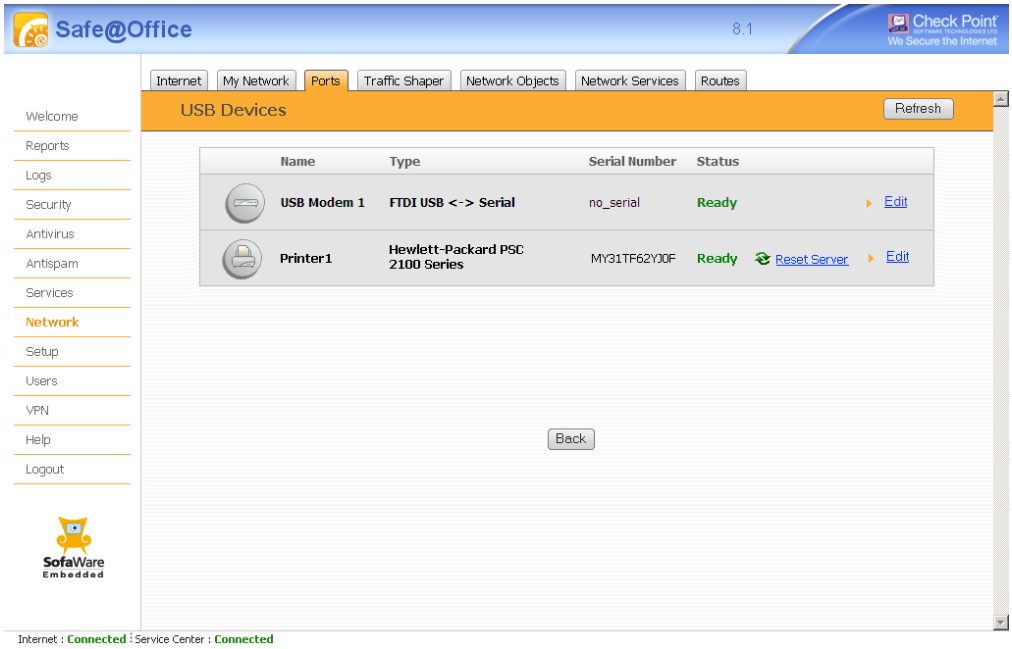
3. In the Safe@Office Portal, click Network in the main menu, and click the Ports tab.

   The Ports page appears.



4. Next to USB, click Edit.

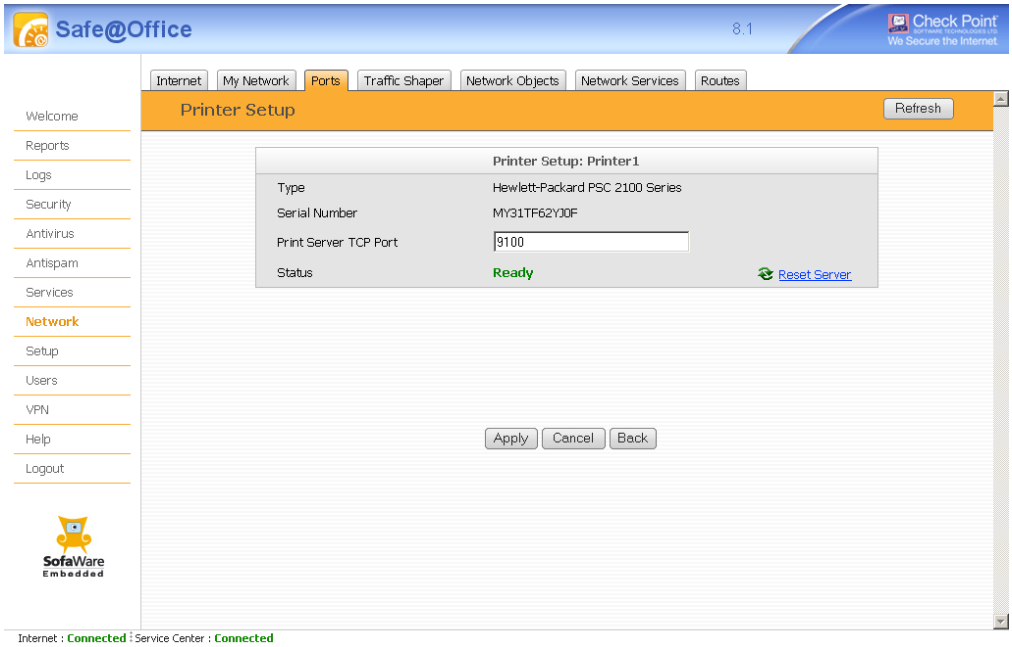
The USB Devices page appears. If the Safe@Office appliance detected the printer, the printer is listed on the page.



If the printer is not listed, check that you connected the printer correctly, then click Refresh to refresh the page.

5. Next to the printer, click Edit.

The Printer Setup page appears.



6. Write down the port number allocated to the printer.

   The port number appears in the Printer Server TCP Port field. You will need this number later, when configuring computers to use the network printer.

7. To change the port number, do the following:

   a. Type the desired port number in the Printer Server TCP Port field.

Note: Printer port numbers may not overlap, and must be high ports.

   b. Click Apply.

   You may want to change the port number if, for example, the printer you are setting up is intended to replace another printer. In this case, you should change the replacement printer's port number to the old printer's port number, and you can skip the next step.

8. Configure each computer from which you want to enable printing to the network printer.

See ***Configuring Computers to Use Network Printers*** on page 771.

Configuring Computers to Use Network Printers

USB

Perform the relevant procedure on each computer from which you want to enable printing via the Safe@Office print server to a network printer.

Windows Vista

This procedure is relevant for computers with a Windows Vista operating system.

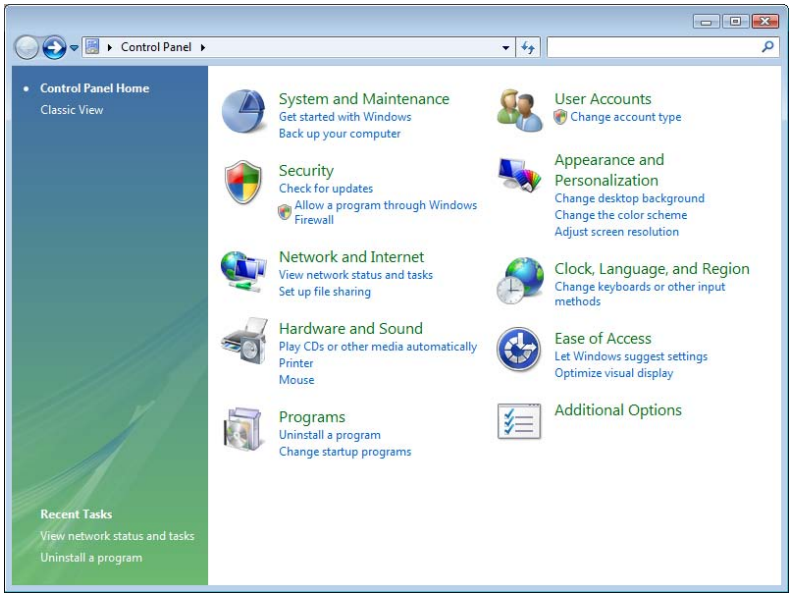
To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 404.

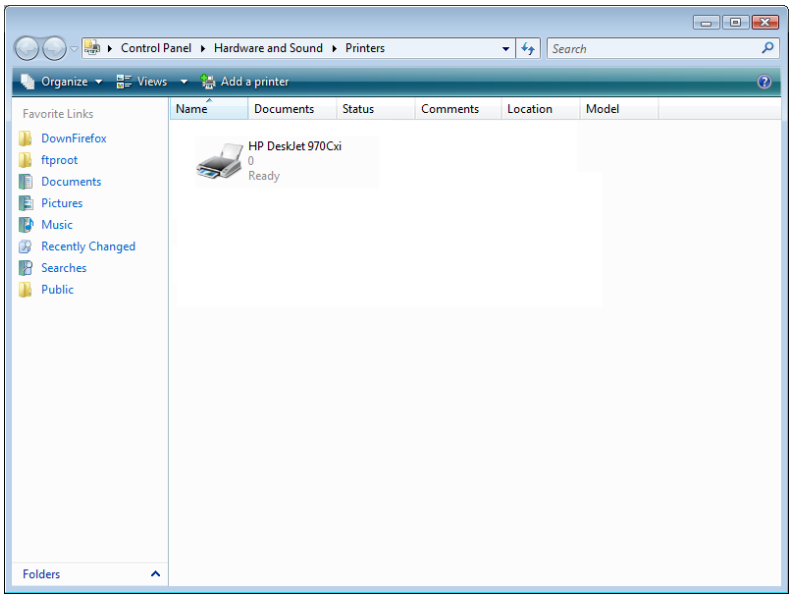
2. Click Start > Control Panel.

The **Control Panel** window opens.



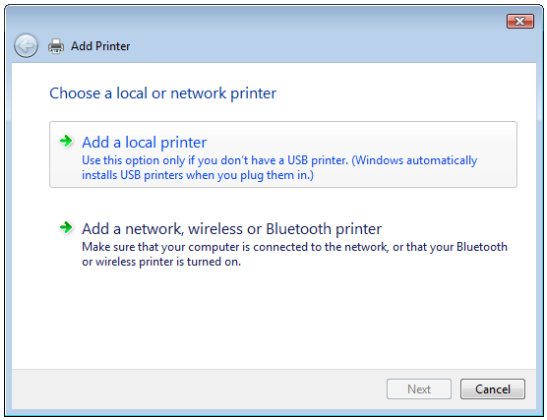
3. Under **Hardware and Sound**, click **Printer**.

The Printers screen appears.



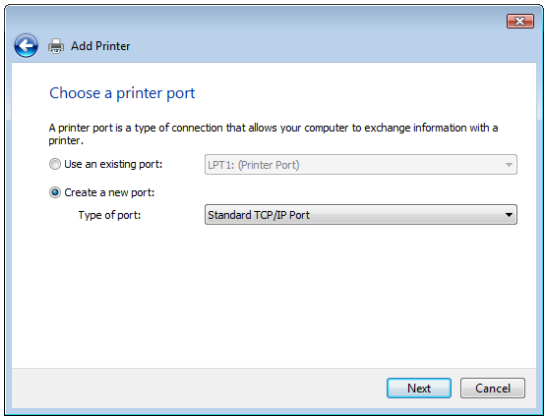
4. Click Add a printer.

   The Add Printer wizard opens displaying the Choose a local or network printer screen.


Add Printer
Choose a local or network printer
Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)
Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.
Next
Cancel

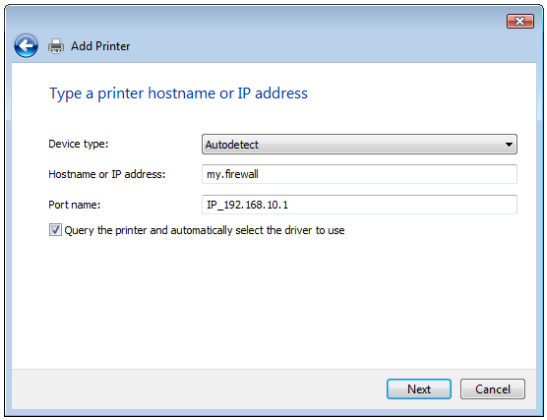
5. Click Add a local printer.
6. Click Next.

The Choose a printer port dialog box appears.


Add Printer
Choose a printer port
A printer port is a type of connection that allows your computer to exchange information with a printer.
Use an existing port:
LPT1: (Printer Port)
Create a new port:
Type of port:
Standard TCP/IP Port
Next
Cancel

7. Click Create a new port.
8. In the Type of port drop-down list, select Standard TCP/IP Port.
9. Click Next.

   The Type a printer hostname or IP address dialog box appears.



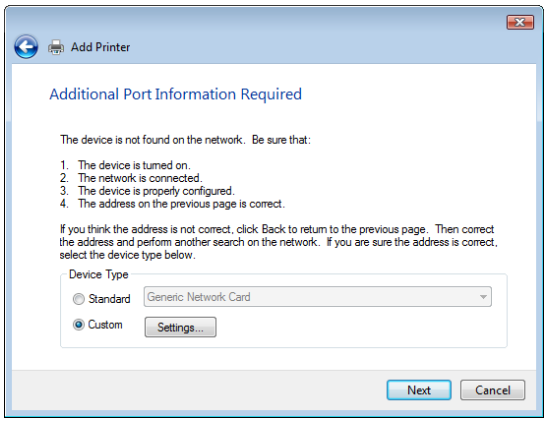
10. In the Device type drop-down list, select Autodetect.
11. In the Hostname or IP address field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

    You can find the LAN IP address in the Safe@Office Portal, under Network > My Network.

12. In the Port name field, type the port name.
13. Select the Query the printer and automatically select the driver to use check box.
14. Click Next.

    The following things happen:

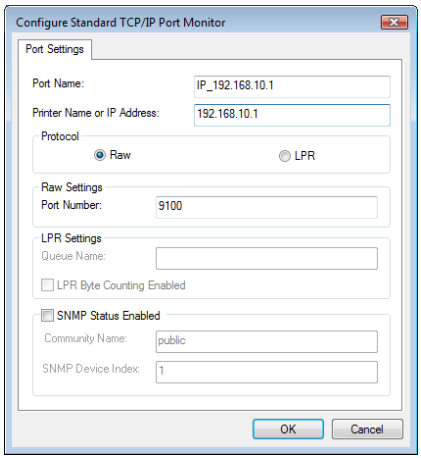
    - If Windows cannot identify your printer, the Additional Port Information Required dialog box appears.


Add Printer
Additional Port Information Required
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
Next
Cancel

    Do the following:

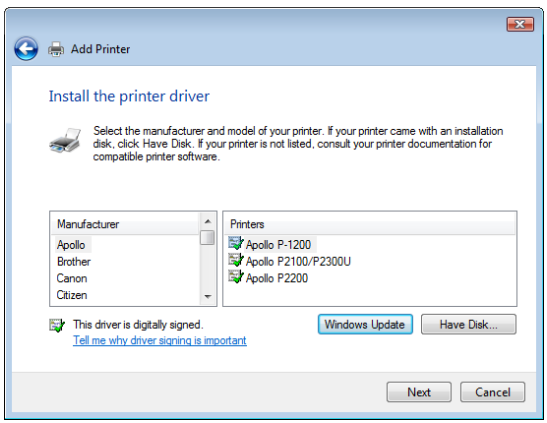
    1) Click Custom.
    2) Click Settings.

The Configure Standard TCP/IP Port Monitor dialog box opens.



3) In the Protocol area, make sure that Raw is selected.
4) In the Port Number field, type the printer's port number, as shown in the Printers page.
5) Click OK.
6) Click Next.

- The Install the printer driver dialog box displayed.



15. Do one of the following:

- Use the lists to select the printer's manufacturer and model.

- If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click Have Disk.

16. Click Next.
17. Complete the remaining dialog boxes in the wizard as desired, and click Finish.

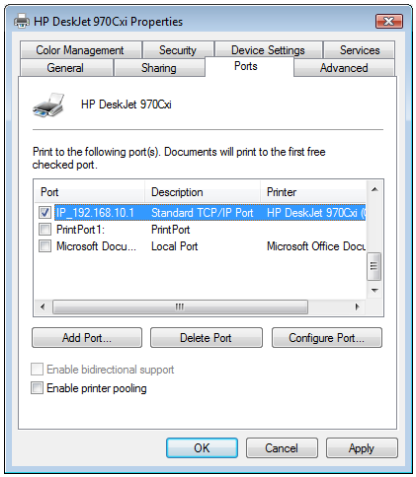
    The printer appears in the Printers and Faxes window.

18. Right-click the printer and click Properties in the popup menu.

    The printer's Properties dialog box opens.

19. In the Ports tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



20. Click OK.

Windows 2000/XP

This procedure is relevant for computers with a Windows 2000/XP operating system.

To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 404.

2. Click Start > Settings > Control Panel.

   The Control Panel window opens.

3. Click Printers and Faxes.

   The Printers and Faxes window opens.

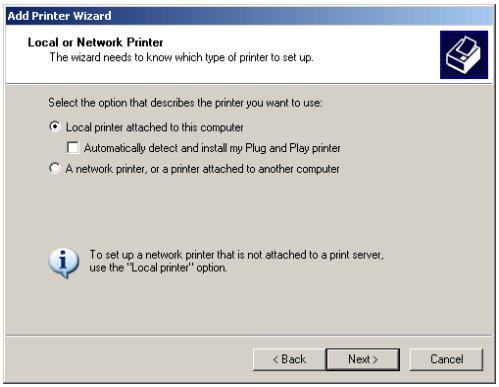
4. Right-click in the window, and click Add Printer in the popup menu.

   The Add Printer Wizard opens with the Welcome dialog box displayed.

Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

5. Click Next.

The Local or Network Printer dialog box appears.

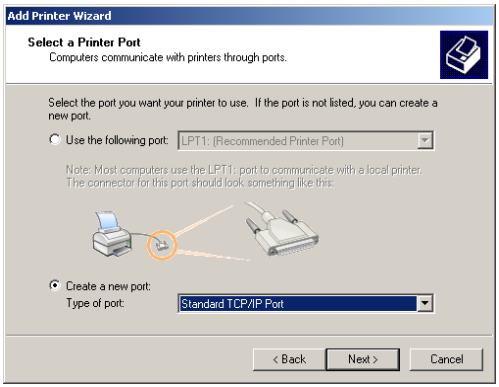

Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

6. Click Local printer attached to this computer.

Note: Do not select the Automatically detect and install my Plug and Play printer check box.

7. Click Next.

   The Select a Printer Port dialog box appears.


Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

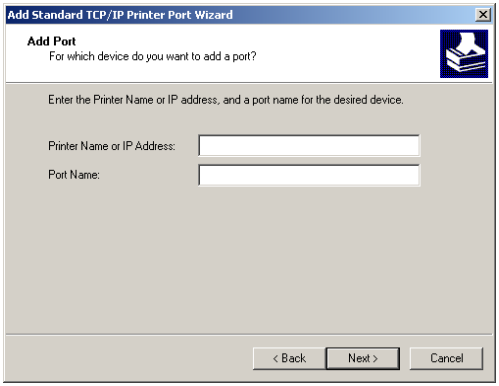
8. Click Create a new port.
9. In the Type of port drop-down list, select Standard TCP/IP Port.
10. Click Next.

The Add Standard TCP/IP Port Wizard opens with the Welcome dialog box displayed.

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

11. Click Next.

    The Add Port dialog box appears.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
Port Name:
< Back
Next >
Cancel

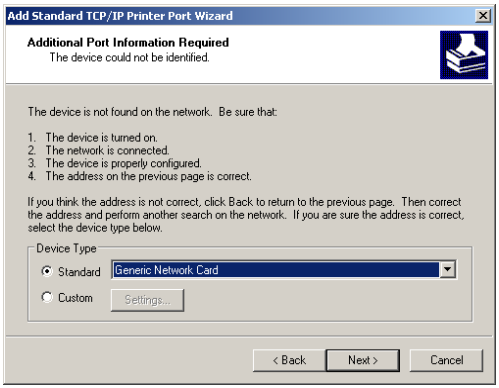
12. In the Printer Name or IP Address field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

    You can find the LAN IP address in the Safe@Office Portal, under Network > My Network.

    The Port Name field is filled in automatically.

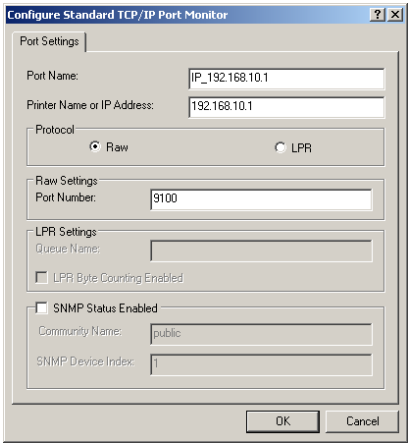
13. Click Next.

The Add Standard TCP/IP Printer Port Wizard opens, with the Additional Port Information Required dialog box displayed.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

14. Click Custom.
15. Click Settings.

    The Configure Standard TCP/IP Port Monitor dialog box opens.

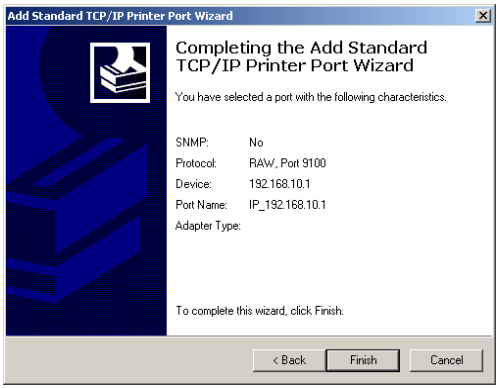


16. In the Port Number field, type the printer's port number, as shown in the Printers page.
17. In the Protocol area, make sure that Raw is selected.
18. Click OK.

    The Add Standard TCP/IP Printer Port Wizard reappears.

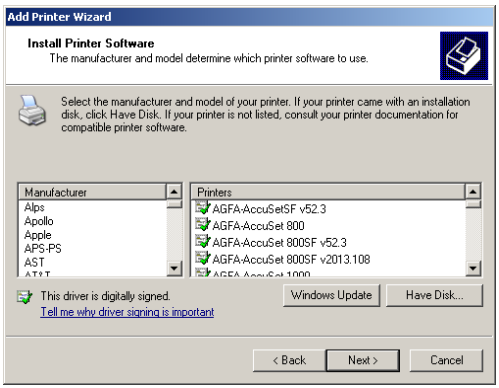
19. Click Next.

    The Completing the Add Standard TCP/IP Printer Port Wizard dialog box appears.



20. Click Finish.

    The Add Printer Wizard reappears, with the Install Printer Software dialog box displayed.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
Alps
Apollo
Apple
APS-PS
AST
Printers
AGFA-AccuSetSF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
AGFA-AccuSet 800SF v2013.108
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

21. Do one of the following:

    - Use the lists to select the printer's manufacturer and model.
    - If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click Have Disk.

22. Click Next.

23. Complete the remaining dialog boxes in the wizard as desired, and click Finish.

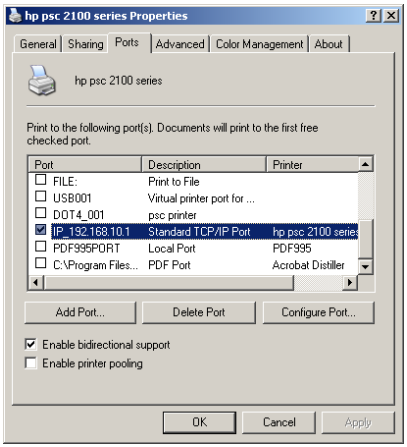
The printer appears in the Printers and Faxes window.

24. Right-click the printer and click Properties in the popup menu.

    The printer's Properties dialog box opens.

25. In the Ports tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



26. Click OK.

MAC OS-X

This procedure is relevant for computers with the latest version of the MAC OS-X operating system.

Note: This procedure may not apply to earlier MAC OS-X versions.

To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

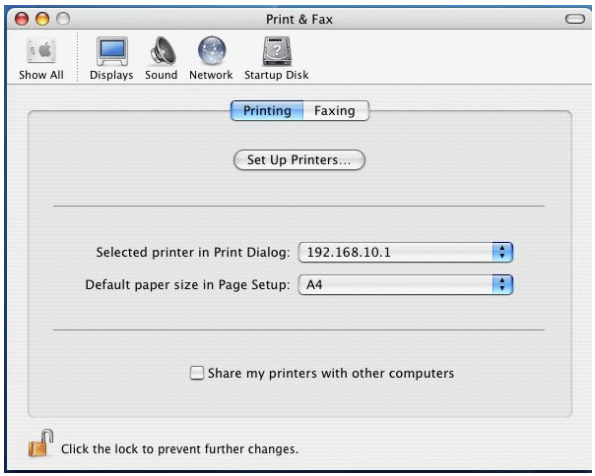
   See ***Adding and Editing Rules*** on page 404.

2. Choose Apple -> System Preferences.

   The System Preferences window appears.

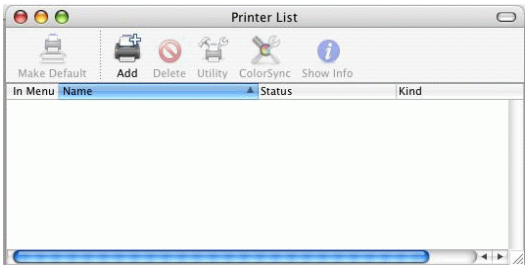
3. Click Show All to display all categories.
4. In the Hardware area, click Print & Fax.

The Print & Fax window appears.



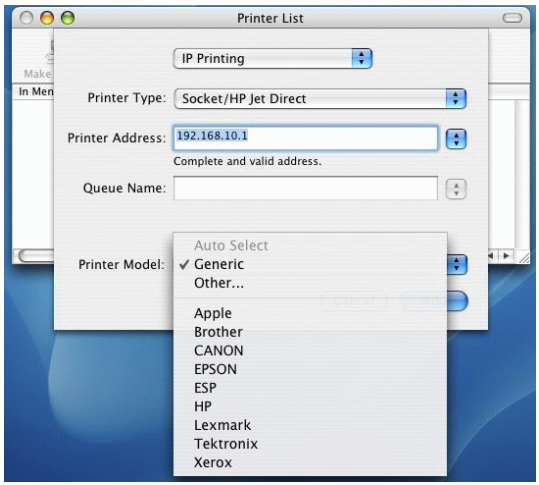
5. In the Printing tab, click Set Up Printers.

   The Printer List window appears.



6. Click Add.

New fields appear.

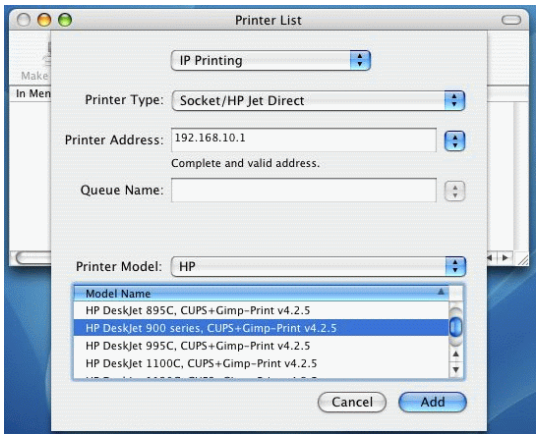


7. In the first drop-down list, select IP Printing.
8. In the Printer Type drop-down list, select Socket/HP Jet Direct.
9. In the Printer Address field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

   You can find the LAN IP address in the Safe@Office Portal, under Network > My Network.
10. In the Queue Name field, type the name of the required printer queue.

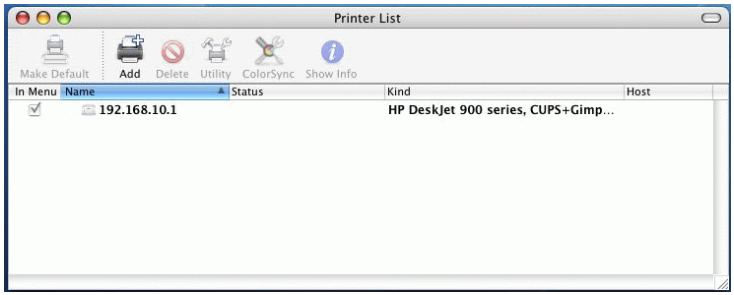
    For example, the printer queue name for HP printers is RAW.
11. In the Printer Model list, select the desired printer type.

A list of models appears.



12. In the Model Name list, select the desired model.
13. Click Add.

    The new printer appears in the Printer List window.



14. In the Printer List window, select the newly added printer, and click Make Default.

Viewing Network Printers

USB

To view network printers

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

   For each printer, the model, serial number, and status is displayed.

   A printer can have the following statuses:

   - Initialize. The printer is initializing.
   - Ready. The printer is ready.
   - Not Ready. The printer is not ready. For example, it may be out of paper.
   - Printing. The printer is processing a print job.
   - Restarting. The printer server is restarting.
   - Fail. An error occurred. See the Event Log for details (***Viewing the Event Log*** on page 379).

3. To refresh the display, click Refresh.

Changing Network Printer Ports

USB

When you set up a new network printer, the Safe@Office appliance automatically assigns a port number to the printer. If you want to use a different port number, you can easily change it, as described in ***Setting Up Network Printers*** on page 768.

However, you may sometimes need to change the port number after completing printer setup. For example, you may want to replace a malfunctioning network printer, with another existing network printer, without reconfiguring the client computers. To do this, you must change the replacement printer's port number to the malfunctioning printer's port number, as described below.

Note: Each printer port number must be different, and must be a high port.

To change a printer's port

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

3. Next to the desired printer, click Edit.

   The Printer Setup page appears.

4. In the printer's Printer Server TCP Port field, type the desired port number.

5. Click Apply.

Resetting Network Printers

USB

You can cause a network printer to restart the current print job, by resetting the network printer. You may want to do this if the print job has stalled.

To reset a network printer

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

3. Next to the desired printer, click Reset Server.

   The network printer's current print job is restarted.

Chapter 25

Troubleshooting

This chapter provides solutions to common problems you may encounter while using the Safe@Office appliance.

Note: For information on troubleshooting wireless connectivity, see ***Troubleshooting Wireless Connectivity*** on page *342*.

This chapter includes the following topics:

Connectivity 791
Service Center and Upgrades..... 795
Other Problems 796

Connectivity

I cannot access the Internet. What should I do?

- Verify that the Safe@Office appliance is operating. If not, check the power connection to the Safe@Office appliance.
- Check if the LED for the WAN port is green. If not, check the network cable to the modem and make sure the modem is turned on.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly. Try replacing the cable or connecting it to a different LAN port.
- Using your Web browser, go to http://my.firewall and see whether "Connected" appears on the Status Bar. Make sure that your Safe@Office appliance network settings are configured as per your ISP directions.
- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 85.
- If Web Filtering or Email Filtering are on, try turning them off.

- Check if you have defined firewall rules which block your Internet connectivity.
- Check with your ISP for possible service outage.
- Check whether you are exceeding the maximum number of computers allowed by your license, by viewing the My Computers page.

I cannot access my DSL broadband connection. What should I do?

DSL equipment comes in two flavors: bridges (commonly known as DSL modems) and routers. Some DSL equipment can be configured to work both ways.

- If you connect to your ISP using a PPPoE or PPTP dialer defined in your operating system, your equipment is most likely configured as a DSL bridge. Configure a PPPoE or PPTP type DSL connection.
- If you were not instructed to configure a dialer in your operating system, your equipment is most likely configured as a DSL router. Configure a LAN connection, even if you are using a DSL connection.

For instructions, see ***Configuring the Internet Connection*** on page 125.

I cannot access my Cable broadband connection. What should I do?

- Some cable ISPs require you to register the MAC address of the device behind the cable modem. You may need to clone your Ethernet adapter MAC address onto the Safe@Office appliance. For instructions, see ***Configuring the Internet Connection*** on page 125.
- Some cable ISPs require using a hostname for the connection. Try reconfiguring your Internet connection and specifying a hostname. For further information, see ***Configuring the Internet Connection*** on page 125.

I cannot access my ADSL connection from an ADSL appliance. What should I do?

- Check that a micro-filter is used on all the phone sockets on the line (required in most locations).
- Check that the DSL Standard setting configured for your appliance is compatible with your service provider. You can view this setting in the Network > Internet Setup page.
- Advanced ADSL configuration fine tuning options are available via the CLI. For information, refer to the *Embedded NGX CLI Reference Guide*.

I cannot access http://my.firewall or http://my.vpn. What should I do?

- Verify that the Safe@Office appliance is operating.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly.
- By default, unencrypted HTTP access is not allowed from the wireless LAN to http://my.firewall or http://my.vpn. Therefore, if you are connecting from the wireless LAN, try connecting to https://my.firewall instead.
- Try surfing to 192.168.10.1 instead of to my.firewall.

Note: 192.168.10 is the default value, and it may vary if you changed it in the My Network page.

- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 85.
- Restart your Safe@Office appliance and your broadband modem by disconnecting the power and reconnecting after 5 seconds.
- If your Web browser is configured to use an HTTP proxy to access the Internet, add my.firewall or my.vpn to your proxy exceptions list.

My network seems extremely slow. What should I do?

- The Ethernet cables may be faulty. For proper operation, the Safe@Office appliance requires STP CAT5 (Shielded Twisted Pair Category 5) Ethernet cables. Make sure that this specification is printed on your cables.
- Your Ethernet card may be faulty or incorrectly configured. Try replacing your Ethernet card.
- There may be an IP address conflict in your network. Check that the TCP/IP settings of all your computers are configured to obtain an IP address automatically.

I changed the network settings to incorrect values and am unable to correct my error. What should I do?

Reset the network to its default settings using the button on the back of the Safe@Office appliance unit. See ***Resetting the Safe@Office Appliance to Defaults*** on page 762.

I am using the Safe@Office appliance behind another NAT device, and I am having problems with some applications. What should I do?

By default, the Safe@Office appliance performs Network Address Translation (NAT). It is possible to use the Safe@Office appliance behind another device that performs NAT, such as a DSL router or Wireless router, but the device will block all incoming connections from reaching your Safe@Office appliance.

To fix this problem, do ONE of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. The Safe@Office appliance can be used as a replacement for your router, unless you need it for some additional functionality that it provides.
- If possible, disable NAT in the router. Refer to the router's documentation for instructions on how to do this.
- If the router has a "DMZ Computer" or "Exposed Host" option, set it to the Safe@Office appliance's external IP address.
- Open the following ports in the NAT device:
  - UDP 9281/9282
  - UDP 500
  - UDP 2746
  - TCP 256
  - TCP 264
  - ESP IP protocol 50
  - TCP 981

I cannot receive audio or video calls through the Safe@Office appliance. What should I do?

To enable audio/video, you must configure an IP Telephony (H.323) virtual server. For instructions, see ***Configuring Servers*** on page 397.

I run a public Web server at home but it cannot be accessed from the Internet. What should I do?

Configure a virtual Web Server. For instructions, see ***Configuring Servers*** on page 397.

I cannot connect to the LAN network from the DMZ or primary WLAN network. What should I do?

By default, connections from the DMZ or primary WLAN network to the LAN network are blocked. To allow traffic from the DMZ or primary WLAN to the LAN, configure appropriate firewall rules. For instructions, see ***Using Rules*** on page 400.

Service Center and Upgrades

I have exceeded my node limit. What does this mean? What should I do?

Your Product Key specifies a maximum number of nodes that you may connect to the Safe@Office appliance.

The Safe@Office appliance tracks the cumulative number of nodes on the internal network that have communicated through the firewall. When the Safe@Office appliance encounters an IP address that exceeds the licensed node limit, the My Computers page displays a warning message and marks nodes over the node limit in red. These nodes will not be able to access the Internet through the Safe@Office appliance, but will be protected. The Event Log page also warns you that you have exceeded the node limit.

To upgrade your Safe@Office appliance to support more nodes, purchase a new Product Key. Contact your reseller for upgrade information.

While trying to connect to a Service Center, I received the message "The Service Center did not respond". What should I do?

- If you are using a Service Center other than the Check Point Service Center, check that the Service Center IP address is typed correctly.
- The Safe@Office appliance connects to the Service Center using UDP ports 9281/9282. If the Safe@Office appliance is installed behind another firewall, make sure that these ports are open.

I purchased an advanced Safe@Office model, but I only have the functionality of a simpler Safe@Office model. What should I do?

Your have not installed your product key. For further information, see ***Upgrading Your Software Product*** on page 722.

Other Problems

I have forgotten my password. What should I do?

Reset your Safe@Office appliance to factory defaults using the Reset button as detailed in ***Resetting the Safe@Office Appliance to Defaults*** on page 762.

Why are the date and time displayed incorrectly?

You can adjust the time on the Setup page's Tools tab. For information, see ***Setting the Time on the Appliance*** on page 735.

I cannot use a certain network application. What should I do?

Look at the Event Log page. If it lists blocked attacks, do the following:

- Set the Safe@Office appliance's firewall level to Low and try again.
- If the application still does not work, set the computer on which you want to use the application to be the exposed host.

  For instructions, see Defining an Exposed Host.

When you have finished using the application, make sure to clear the exposed host setting, otherwise your security might be compromised.

In the Safe@Office Portal, I do not see the pop-up windows that the guide describes. What should I do?

Disable any pop-up blockers for http://my.firewall.

Chapter 26

Specifications

This chapter includes the following topics:

Technical Specifications 797
CE Declaration of Conformity 807

Technical Specifications

Safe@Office 1000N and 1000NW

ADSL Model Attributes

Table 159: Safe@Office ADSL Model Attributes

Attribute	Safe@Office 1000N ADSL SBXNDEF-100-2	Safe@Office 1000NW ADSL SBXNWDE-100-2
Physical Attributes		
Dimensions (width x height x depth)	20 x 3.1 x 12.8 cm	20 x 3.1 x 12.8 cm
Weight	805g. (full / packaged 1560g)	850g. (full / packaged 1625g)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm	290 x 250 x 80 mm
Power Adapter Unit		
Power Adapter Nominal Input	In: 100~240VAC @ 0.65A	In: 100~240VAC @ 0.65A

Power Adapter Nominal Output	12VDC @ 2 A	12VDC @ 2 A
Max. Power Consumption	15W 20W (including USB devices)	15W 20W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-20ºC ~ 70ºC	-20ºC ~ 70ºC
Temperature: Operation	0ºC ~ 35ºC	0ºC ~ 35ºC
Humidity: Storage/Operation	10 ~ 90% / 10 ~ 90% (non-condensed)	10 ~ 90% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	TBD	TBD
Quality	TBD	TBD
EMC	TBD	TBD
Reliability	TBD	TBD
Environment	TBD	TBD
MTBF (hours)	TBD	TBD
RF	TBD	TBD

Non-ADSL Model Attributes

Table 160: Safe@Office Non-ADSL Model Attributes

Attribute	Safe@Office 1000N SBXN-100-1	Safe@Office 1000NW SBXNW-100-1
Physical Attributes		
Dimensions (width x height x depth)	20 x 3.1 x 12.8 cm (7.87 x 1.22 x 5.04 inches)	20 x 3.1 x 12.8 cm (7.87 x 1.22 x 5.04 inches) (excluding antenna connectors)
Weight	750g. (full / packaged 1505g)	770g. (full / packaged 1545g)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
Power Adapter Unit		
Power Adapter Nominal Input	In: 100~240VAC @ 0.65A	In: 100~240VAC @ 0.65A
Power Adapter Nominal Output	12VDC @ 2 A	12VDC @ 2 A
Max. Power Consumption	12W	16W 21W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-20÷C ~ 70÷C	-20÷C ~ 70÷C
Temperature: Operation	0÷C ~ 35÷C	0÷C ~ 35÷C

Humidity: Storage/Operation	10 ~ 90% / 10 ~ 90% (non-condensed)	10 ~ 90% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	cULus, CB, CE, LVD	cULus, CB, CE, LVD
Quality	ISO9001, ISO 14001, TL9000	ISO9001, ISO 14001, TL9000
EMC	CE, FCC 15B	CE, FCC 15B
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE, China RoHS	RoHS & WEEE, China RoHS
MTBF (hours)	100,000 hours at 25÷C	100,000 hours at 25÷C
RF	N/A	CE R&TTE .FCC15C,TELCO

Wireless Attributes

Table 161: Safe@Office Wireless Attributes

Attribute	Safe@Office 1000NW SBXNW-100-1 Safe@Office 1000NW ADSL SBXNWDE-100-2		
Operation Frequency	2.412-2.484 MHz		
Transmission Power	**Mode**	**dBm**	**mW**
	802.11b	16	40mW
	802.11g	11 (54Mbps), 16 (6Mbps)	13mW (54Mbps), 40mW (6Mbps)
	802.11n (HT20)	9 (MCS7, MCS15), 16 (MCS0)	8mW (MCS7, MCS15), 40mW (MCS0)
	802.11n (HT40)	8 (MCS7, MCS15), 16 (MCS0)	6.3mW (MCS7, MCS15), 40mW (MCS0)
	50mW Max		
Modulation	OFDM, DSSS, 64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK, DBPSK		
WPA Authentication Modes	EAP-TLS, EAP-TTLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2)		

Safe@Office 500 and 500W

Table 162: Safe@Office ADSL Models Attributes

Attribute	Safe@Office 500 ADSL SBXD-166LHGE-5	Safe@Office 500W ADSL SBXWD-166LHGE-5
Physical Attributes		
Dimensions (width x height x depth)	200 x 33 x 122 mm (7.87 x 1.3 x 4.8 inches)	200 x 33 x 130 mm (7.87 x 1.3 x 5.12 inches) (incl. antenna connectors)
Weight	660 g (1.46 lbs)	694 g (1.53 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
5V Power Adapter Unit		
Power Adapter Nominal Input	In: 100~240VAC @ 0.5A	In: 100~240VAC @ 0.5A
Power Adapter Nominal Output	5V DC @ 3.3A	5V DC @ 3.3A
Max. Power Consumption	8.5W 13.5W (including USB devices)	10.5W 15.5W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-5÷C ~ 80÷ C	-5÷C ~ 80÷C

Temperature: Operation	0÷C ~ 40÷C	0÷C ~ 40÷C
Humidity: Storage/Operation	10 ~ 95% / 10 ~ 90% (non-condensed)	10 ~ 95% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	cULus, CB, LVD	cULus, CB, LVD
Quality	ISO9001, ISO 14001, TL9000	ISO9001, ISO 14001, TL9000
EMC	CE . FCC 15B.VCCI	CE . FCC 15B.VCCI
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE
ADSL	FCC Part 68.CS03	FCC Part 68.CS03
RF	N/A	FCC15C, TELCO

Table 163: Safe@Office Non-ADSL Models Attributes

Attribute	Safe@Office 500 SBX-166LHGE-5	Safe@Office 500W SBXW-166LHGE-5
Physical Attributes		
Dimensions (width x height x depth)	200 x 33 x 122 mm (7.87 x 1.3 x 4.8 inches)	200 x 33 x 130 mm (7.87 x 1.3 x 5.12 inches) (incl. antenna connectors)
Weight	580 g (1.28 lbs)	635 g (1.40 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)

5V Power Adapter Unit		
Power Adapter Nominal Input	In: 100~240VAC @ 0.5A	In: 100~240VAC @ 0.5A
Power Adapter Nominal Output	9VAC @ 1.5 A OR: 12VDC @ 1.5 A	12VDC @ 1.5 A
Max. Power Consumption	4.5W	6.5W 11.5W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-5÷C ~ 80÷C	-5÷C ~ 80÷C
Temperature: Operation	0÷C ~ 40÷C	0÷C ~ 40÷C
Humidity: Storage/Operation	10 ~ 95% / 10 ~ 90% (non-condensed)	10 ~ 95% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	cULus, CB, LVD	cULus, CB, LVD
Quality	ISO9001, ISO 14001, TL9000	ISO9001, ISO 14001, TL9000
EMC	CE . FCC 15B.VCCI	CE . FCC 15B.VCCI
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE
MTBF (hours)	68,000 hours at 30÷C	68,000 hours at 30÷C

RF	N/A	FCC15C,TELCO

Table 164:

Table 165: Safe@Office Non-ADSL Models Attributes

Attribute	Safe@Office 500 SBX-166LHGE-6	Safe@Office 500W SBXW-166LHGE-6
Physical Attributes		
Dimensions (width x height x depth)	200 x 32 x 128 mm (7.87 x 1.26 x 5.04 inches)	200 x 32 x 128 mm (7.87 x 1.26 x 5.04 inches)
Weight	675 g (1.49 lbs)	685 g (1.51 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
Retail box weight	1.36 kg (3 lbs)	1.38 kg (3.04 lbs)
5V Power Adapter Unit		
Power Adapter Nominal Input	100 to 240 Vac 50 to 60 Hz	100 to 240 Vac 50 to 60 Hz
Power Adapter Nominal Output	12VDC @ 1.5 A	12VDC @ 1.5 A
Max. Power Consumption	15W	15W 20W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-20ºC ~ 65ºC	-20ºC ~ 65ºC

Temperature: Operation	0ºC ~ 40ºC	0ºC ~ 40ºC
Humidity: Storage/Operation	10% ~ 85% (non-condensed)	10% ~ 85% (non-condensed)
Applicable Standards		
Safety	IEC 60950, EN 60950	IEC 60950, EN 60950
Quality	ISO 9001, 9002, 14001	ISO 9001, 9002, 14001
EMC	FCC part 15B VCCI V-3/V-4	FCC Part 15 B & C AS/NZS 4268: 2003 A1 DGT
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE
MTBF (hours)	68,000 hours at 30ºC	68,000 hours at 30ºC
RF	N/A	CE, FCC15C, TELCO

Wireless Attributes

Table 166: Safe@Office Wireless Attributes

Attribute	All Wireless Models
Operation Frequency	2.412-2.484 MHz
Transmission Power	79.4 mW
Modulation	OFDM, DSSS, 64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK,

	DBPSK
WPA Authentication Modes	EAP-TLS, EAP-TTLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2)

CE Declaration of Conformity

CE

Check Point is committed to protecting the environment. Safe@Office unified threat management appliances are compliant with the RoHS Directive, meeting the European Union's strict restrictions on hazardous substances.

RoHS & WEEE Declaration and Certification

The Safe@Office appliance has been verified to comply with the following directives, throughout the design, development, and supply chain stages:

- Directive of the European Parliament and of the Council, of 27 January 2003, on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS – 2002/95/EC)
- Directive of the European Parliament and of the Council, of 27 January 2003, on Waste Electrical and Electronic Equipment (WEEE – 2002/96/CE)

For a copy of the original signed declaration (in full conformance with EN45014), contact SofaWare technical support at www.sofaware.com/support.

SofaWare Technologies Ltd., 3 Hilazon St., Ramat-Gan Israel, hereby declares that this equipment is in conformity with the essential requirements specified in Article 3.1 (a) and 3.1 (b) of:

- Directive 89/336/EEC (EMC Directive)
- Directive 73/23/EEC (Low Voltage Directive – LVD)
- Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive)

In accordance with the following standards:

Table 167: Safe@Office CE Compliance Standards

Attribute	500	500 ADSL	500W ADSL	500W
H/W Model	SBX-166LHGE-5	SBX-166LHGE-5	SBX-166LHGE-5	SBX-166LHGE-6
EMC:	V	V	V	V
EN 55022	V	V	V	
EN 50081-1				V
EN 50082-1				V
EN 61000-3-2	V	V	V	V
EN 61000-3-3	V	V	V	V
EN 55024	V	V	V	V
CISPR 22	V	V	V	V
Safety:	V	V	V	V
EN 60950	V	V	V	V
IEC 60950	V	V	V	V
Telecom:		V	V	
ITU-T G.992.1, .2, .3*, .4*		V	V	

Attribute	500	500 ADSL	500W ADSL	500W
ETSI TS 101 388		V	V	
ITU-T G.703		V	V	
ITU-T G.704		V	V	
RF:				V
EN 300 328				V
EN 301 489-1				V
EN 301 489-17				V
EN 50385				V

Table 168: Safe@Office CE Compliance Standards

Attribute	1000N	1000NW	1000N ADSL	1000NW ADSL
H/W Model	SBXN-100-1	SBXNW-100-1	SBXNDEF-100-2	SBXNWDE-100-2
EMC:				
EN 55022	V	V	V	V

Attribute	1000N	1000NW	1000N ADSL	1000NW ADSL
EN 61000-3-2	V	V	V	V
EN 61000-3-3	V	V	V	V
EN 55024	V	V	V	V
CISPR 22	V	V	V	V
Safety:				
EN 60950	V	V	V	V
IEC 60950	V	V	V	V
Telecom:				
TBR21			V	V
ITU-T G.992.1, .2, .3*, .4*			V	V
ETSI TS 101 388			V	V
ITU-T G.703			V	V
ITU-T G.704			V	V
RF:				

Attribute	1000N	1000NW	1000N ADSL	1000NW ADSL
EN 300 328		V		V
EN 301 489-1		V		V
EN 301 489-17		V		V
EN 50385		V		V

The "CE" mark is affixed to this product to demonstrate conformance to the R&TTE Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive) and FCC Part 15 Class B.

The product has been tested in a typical configuration. For a copy of the Original Signed Declaration (in full conformance with EN45014), please contact SofaWare at the above address.

North America

Federal Communications Commission Radio Frequency Interference Statement

This equipment complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

Any changes or modifications to this product not explicitly approved by the manufacturer could void the user's authority to operate the equipment and any assurances of Safety or Performance, and could result in violation of Part 15 of the FCC Rules.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

FCC Radiation Exposure Statement for Wireless Models

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons. This equipment must not be operated in conjunction with any other antenna.

Table 169: Safe@Office North America Compliance Standards

Attribute	500	500 ADSL	500W ADSL	500W
H/W Model	SBX-166LHGE-5	SBX-166LHGE-5	SBX-166LHGE-5	SBX-166LHGE-6
EMC:	V	V	V	V
FCC Part 15, Class B	V	V	V	V
CISPR 22	V	V	V	V
ICES-003	V	V	V	V
ANSI C63.4	V	V	V	V
Safety:	V	V	V	V
UL 60950	V	V	V	V

Attribute	500	500 ADSL	500W ADSL	500W
C22.2 No. 60950	V	V	V	V
K60950	V	V	V	V
Telecom:				
FCC Part 68		V	V	
TIA-968-A-1, 2 & 3		V	V	
CS-03 Part I & VIII Issue 8		V	V	
RF:				
FCC Part 15, Subpart C				V
IEEE C95.1				V

Table 170: Safe@Office North America Compliance Standards

Attribute	1000N	1000NW	1000N ADSL	1000NW ADSL
H/W Model	SBXN-100-1	SBXNW-100-1	SBXNDEF-100-2	SBXNWDE-100-2

Attribute	1000N	1000NW	1000N ADSL	1000NW ADSL
EMC:				
FCC Part 15, Class B	V	V	V	V
CISPR 22	V	V	V	V
ICES-003	V	V	V	V
ANSI C63.4	V	V	V	V
Safety:				
UL 60950	V	V	V	V
C22.2 No. 60950	V	V	V	V
Telecom:				
FCC Part 68			V	V
CS-03 Part I & VIII Issue 8			V	V
RF:				
FCC Part 15, Subpart C		V		V
IEEE C95.1		V		V

China

China RoHS, RoHS & WEEE Declaration and Certification

These systems have been verified to comply with the China RoHS and EU RoHS & WEEE Directives throughout the design, development and supply chain definition.

China RoHS, RoHS & WEEE

(Environmental Data – Product's Materials Information Restricted Substances)

SofaWare's products does NOT contain any of the following substances (in concentrations exceeding legal threshold limits):

- Asbestos
- Colorants in components that come into direct contact with human skin
- Cadmium and its compounds (except for use in applications exempted by the EU RoHS Directive)
- Class I and Class II CFCs (chlorofluorocarbons) and HCFCs (hydro fluorocarbons)
- Chloroparaffins, short chained (10-13 carbon chain)
- Chromium VI and its compounds (except for use in applications exempted by the EU RoHS Directive)
- Halogenated dioxins or furans (i.e. polychlorinated dibenzodioxines, polychlorinated dibenzofurans)
- Lead and its compounds (except for use in applications exempted by the EU RoHS Directive)
- Mercury (except for use in applications exempted by the EU RoHS Directive)
- Nickel and its compounds in components that are likely to result in prolonged skin exposure
- PCBs (polychlorobiphenyls) or PCTs (polychloroterphenyls)
- PBBs (polybromobiphenyls) or PBDEs (polybrominated diphenylethers)
- PVC (polyvinyl chloride) in plastic parts greater than 25 grams
- Polychlorinated naphthalenes (PCNs)

- Tributyl tin (TBT) and triphenyl tin (TPT) compounds

Additional Materials Information

- The cables may use PVC as an insulating material to ensure product safety
- The case material is sheet metal
- Product may contain post-industrial recycled content (plastics, metal, glass)

No CFCs (chlorofluorocarbons), HCFCs (hydrofluorocarbons) or other ozone depleting substances are used in packaging material. Chromium, lead, mercury, or cadmium are not intentionally added to packaging materials and are not present in a cumulative concentration greater than 100 ppm as incidental impurities. No halogenated plastics or polymers are used for packaging material. The System fully complies with the EU Directive 94/62/EEC.

Table 171: Hazardous Substances in Components

Component Name	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Chromium VI Compounds (Cr 6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB	O	O	O	O	O	O
Components onboard	See the following table	O	O	O	O	O
Main Chassis	O	O	O	O	O	O

AC Mains	O	O	O	O	O	O
Accessories	O	O	O	O	O	O
Cables	O	O	O	O	O	O

Table 172: Onboard Components - Lead (Pb)

Component Name	Part	Hazardous Substances	Concentration (ppm)	RoHS Exemptions	Quantity
Components onboard	DC Jack	Lead (Pb)	36050	Lead as an alloying element in steel containing up to 0,35 % lead by weight, aluminium containing up to 0,4 % lead by weight and as a copper alloy containing up to 4 % lead by weight. (2002/95/EC)	1

	Crystal	Lead (Pb)	11800	Lead in high melting temperature type solders (i.e. lead-based alloys containing 85 % by weight or more lead). (2005/747/EC)	1
	CAPACITOR	Lead (Pb)	6551	Lead in electronic ceramic parts (e.g. piezoelectronic devices) (2002/95/EC)	2
	CAPACITOR	Lead (Pb)	6981	Lead in electronic ceramic parts (e.g. piezoelectronic devices) (2002/95/EC)	1

Glossary of Terms

A

ADSL Modem

A device connecting a computer to the Internet via an existing phone line. ADSL (Asymmetric Digital Subscriber Line) modems offer a high-speed 'always-on' connection.

C

CA

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cable Modem

A device connecting a computer to the Internet via the cable television network. Cable modems offer a high-speed 'always-on' connection.

Certificate Authority

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cracking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

D

DHCP
Any machine requires a unique IP address to connect to the Internet using Internet Protocol. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that assigns Internet Protocol (IP) addresses to computers on the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer.

DMZ
A DMZ (demilitarized zone) is an internal network defined in addition to the LAN network and protected by the Safe@Office appliance.

DNS
The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

Domain Name System
Domain Name System. The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

E

Exposed Host
An exposed host allows one computer to be exposed to the Internet. An example of using an exposed host would be exposing a public server, while preventing outside users from getting direct access form this server back to the private network.

F

Firmware
Software embedded in a device.

G

Gateway
A network point that acts as an entrance to another network.

H

Hacking
An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

A protocol for accessing a secure Web server. It uses SSL as a sublayer under the regular HTTP application. This directs messages to a secure port number rather than the default Web port number, and uses a public key to encrypt data

HTTPS is used to transfer confidential user information.

Hub

A device with multiple ports, connecting several PCs or network devices on a network.

I

IP Address

An IP address is a 32-bit number that identifies each computer sending or receiving data packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP Spoofing

A technique where an attacker attempts to gain unauthorized access through a false source address to make it appear as though communications have originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be masquerading as a local packet with the source IP address of an internal host. The firewall can protect against IP spoofing attacks by limiting network access based on the gateway interface from which data is being received.

IPSEC

IPSEC is the leading Virtual Private Networking (VPN) standard. IPSEC enables individuals or offices to establish secure communication channels ('tunnels') over the Internet.

ISP

An ISP (Internet service provider) is a company that provides access to the Internet and other related services.

L

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single server within a small geographic area.

M

MAC Address
The MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet from your computer, a mapping relates your IP address to your computer's physical (MAC) address on the LAN.

Mbps
Megabits per second. Measurement unit for the rate of data transmission.

MTU
The Maximum Transmission Unit (MTU) is a parameter that determines the largest datagram than can be transmitted by an IP interface (without it needing to be broken down into smaller units). The MTU should be larger than the largest datagram you wish to transmit un-fragmented. Note: This only prevents fragmentation locally. Some other link in the path may have a smaller MTU - the datagram will be fragmented at that point. Typical values are 1500 bytes for an Ethernet interface or 1452 for a PPP interface.

N

NAT
Network Address Translation (NAT) is the translation or mapping of an IP address to a different IP address. NAT can be used to map several internal IP addresses to a single IP address, thereby sharing a single IP address assigned by the ISP among several PCs.

Check Point FireWall-1's Stateful Inspection Network Address Translation (NAT) implementation supports hundreds of pre-defined applications, services, and protocols, more than any other firewall vendor.

NetBIOS
NetBIOS is the networking protocol used by DOS and Windows machines.

P

Packet
A packet is the basic unit of data that flows from one source on the Internet to another destination on the Internet. When any file (e-mail message, HTML file, GIF file etc.) is sent from one place to another on the Internet, the file is divided into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file at the receiving end.

PPPoE
PPPoE (Point-to-Point Protocol over Ethernet) enables connecting multiple computer users on an Ethernet local area network to a remote site or ISP, through common customer premises equipment (e.g. modem).

PPTP

The Point-to-Point Tunneling Protocol (PPTP) allows extending a local network by establishing private "tunnels" over the Internet. This protocol it is also used by some DSL providers as an alternative for PPPoE.

R

RJ-45

The RJ-45 is a connector for digital transmission over ordinary phone wire.

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks.

S

Server

A server is a program (or host) that awaits and requests from client programs across the network. For example, a Web server is the computer program, running on a specific host, that serves requested HTML pages or files. Your browser is the client program, in this case.

Stateful Inspection

Stateful Inspection was invented by Check Point to provide the highest level of security by examining every layer within a packet, unlike other systems of inspection. Stateful Inspection extracts information required for security decisions from all application layers and retains this information in dynamic state tables for evaluating subsequent connection attempts. In other words, it learns!

Subnet Mask

A 32-bit identifier indicating how the network is split into subnets. The subnet mask indicates which part of the IP address is the host ID and which indicates the subnet.

T

TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network.

At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol of the Internet.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end.

UDP is often used for applications such as streaming data.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is 'http://www.sofaware.com'.

V

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VPN tunnel

A secure connection between a Remote Access VPN Client and a Remote Access VPN Server.

W

WLAN

A WLAN is a wireless local area network protected by the Safe@Office appliance.

Index

8

802.1x
- configuring for a wireless network • 309
- configuring for ports • 411
- excluding network objects from • 225

A

Access Denied page
- customizing • 578

account
- configuring • 595

ADSL
- configuring a direct connection • 123

ADSL modem
- about • 817

antispam filtering solutions
- about • 504
- comparison of • 504
- Email Antivirus • 556
- VStream Antispam • 523

antivirus filtering solutions
- about • 503
- Email Antivirus • 556
- solutions • 503
- VStream Antivirus • 505

B

backup connection
- configuring • 189

Block Known Ports • 485

Block List engine
- adding senders • 537
- configuring settings • 539
- deleting senders • 539
- enabling/disabling • 529

Block Port Overflow • 486

Blocked FTP Commands • 487

bridges
- adding and editing • 264
- adding connections to • 272
- adding networks to • 268
- deleting • 276
- explained • 257
- multiple • 262
- using • 257

C

CA, explained • 654, 817

cable modem
- configuring a connection • 123
- explained • 817

certificate
explained • 654
exporting • 663
exporting CA • 664
exporting device • 663
generating self-signed • 655
importing • 659
installing • 654
uninstalling • 662
Checksum Verification • 473
Cisco IOS DOS • 470
command line interface
controlling the appliance via • 707
Content Based Antispam engine
configuring • 533
enabling/disabling • 529

D

DDoS Attack • 461
DHCP
configuring • 198
connection • 132
explained • 818
options • 204
DHCP Server
enabling/disabling • 198
explained • 198
diagnostic tools
Packet Sniffer • 738
Ping • 735
Traceroute • 735
using • 735
WHOIS • 735
diagnostics
running • 762
dialup
connection • 164
RS232 modem • 175
USB modem • 179
direct ADSL connection • 135, 142
DMZ
configuring • 209
configuring High Availability for • 279
explained • 818
DNS • 189, 735, 818
Dynamic DNS • 26, 593

E

EAP authenticator
explained • 431
using with wired clients • 433
using with wireless clients • 432
workflows • 432
Email Antispam, see Email Filtering • 556
Email Antivirus, see Email Filtering • 556
Email Filtering

Email Antispam • 556
Email Antivirus • 556
enabling/disabling • 557
selecting protocols for • 558
snoozing • 559
temporarily disabling • 559
EoA
configuring a connection • 123
Event Log
viewing • 377
exposed host
defining a computer as • 395
explained • 818

F

File and Print Sharing • 490
firewall
about • 389
levels • 392
rule types • 400
setting security level • 392
technologies • 76
firewall rules
adding and editing • 402
deleting • 411
enabling/disabling • 409
enabling/disabling logging • 410
reordering • 410
types • 402
using • 398
firmware
explained • 818
updating • 581
updating by using Software Updates • 582
updating manually • 584
viewing status • 716
Flags • 480
FTP Bounce • 484

G

gateway hostname
configuring • 720
gateways
backup • 279
default • 239
explained • 818
ID • 593
master • 279

H

H.323 • 495
Header Rejection • 488
Hide NAT
enabling/disabling • 197
explained • 197
high availability

configuring • 279
explained • 279
Host Port Scan • 481
HTTPS
configuring • 724
explained • 819
using • 116
hub • 99, 189, 279, 789, 819

I

IGMP • 492
IKE traces
viewing • 668
installation
ADSL models • 100
cable type • 99
network • 99
non-ADSL models • 99
software requirements • 26
Instant Messengers • 498
internal DNS Server
about • 222
configuring • 222
internal VPN Server
configuring • 606
explained • 602
Internet connection
configuring • 123
configuring backup • 189
enabling/disabling • 188
establishing quick • 188
terminating • 188
troubleshooting • 789
viewing information • 186
Internet Setup
using • 139
Internet Wizard
using • 124
IP address
changing • 196
explained • 819
hiding • 197
IP Fragments • 466
IP Reputation engine
configuring • 542
enabling/disabling • 529
IPoA
configuring a connection • 149
ISP
explained • 819

L

L2TP VPN Clients
configuring • 610
L2TP VPN Server
about • 603

configuring • 608
LAN
cable • 99
configuring a connection • 123
configuring High Availability for • 279
explained • 819
ports • 99
LAND • 459
licenses
upgrading • 718
link configurations
modifying • 254
load balancing
about • 190
configuring • 190
login
initial • 111
regular • 114
logs
event logs • 377
exporting • 377
security logs • 381
viewing • 377

M

MAC address
explained • 820
Max Ping Size • 465
MTU
explained • 820

N

NAT rules
about • 423
adding and editing • 425
types • 424
using • 423
viewing and deleting • 430
NetBIOS
explained • 820
network
changing internal range of • 196
configuring • 193
configuring a DMZ • 209
configuring a virtual access point (VAP) • 331
configuring a VLAN • 214
configuring DHCP options • 204
configuring high availability • 279
configuring the OfficeMode network • 212
configuring the WLAN • 303
enabling DHCP Server on • 198
enabling Hide NAT • 197
installation on • 99
managing • 193
objects • 225

Network Interface Monitor
viewing bridge statistics • 370
viewing general network statistics • 360
viewing Internet connection statistics • 361
viewing wired network statistics • 366
viewing wireless network statistics • 368
network objects
adding and editing • 227
using • 225
viewing and deleting • 235
Network Quota • 468
network service objects
adding and editing • 236
viewing and deleting • 238
node limit
viewing • 355
Non-TCP Flooding • 460
Null Payload • 472

O

OfficeMode
about • 212
configuring • 212

P

packet • 186, 239, 735, 819, 820
Packet Sanity • 463
Packet Sniffer
filter string syntax • 741
using • 738
password
changing • 673
setting up • 111
Peer to Peer • 496
Ping of Death • 458
Port-based VLAN
about • 214
adding and editing • 218
deleting • 221
ports
configuring 802.1x security scheme for • 411
managing • 244
modifying assignments • 252
modifying link configurations • 254
resetting to defaults • 255
viewing statuses • 245
PPPoA
configuring a connection • 123
PPPoE
connection • 123
explained • 820
PPTP
connection • 123
explained • 821
primary WLAN

configuring • 303
defined • 822
printers
changing ports • 787
configuring computers to use • 769
resetting • 788
setting up • 766
using • 765
viewing • 786

Q

QoS
classes • 291
explained • 291
QoS classes
adding and editing • 296
assigning services to • 398
deleting • 300
explained • 291
predefined • 294
restoring defaults • 301

R

RADIUS
configuring VSA • 690
explained • 684
using • 684
rapid deployment
about • 756
performing • 758
preparing for • 757
Remote Access VPN Clients
Remote Access VPN Clients • 597
Remote Access VPN Servers
configuring • 603
explained • 597
Remote Desktop
accessing a remote desktop • 703
configuring • 697
configuring the host computer • 700
using • 695
reports
active computers • 355
active connections • 357
network statistics • 360
node limit • 355
routing table • 372
Safe@Office appliance status • 343
traffic • 350
viewing • 343
wireless statistics • 368
routers • 189, 279, 735, 789, 821
RS232 dialup modem
setting up • 175
rules
firewall • 398

NAT • 423
VStream Antispam • 545
VStream Antivirus • 509
Web • 563

S

Safe Senders
adding • 553
deleting • 554
Safe@Office <OLD500><OLDEX>
front panel • 53
network requirements • 51
package contents • 51
rear panel • 51
Safe@Office <OLD500ADSL><OLDEXADSL>
front panel • 58
network requirements • 55
package contents • 55
rear panel • 56
Safe@Office <OLD500W><OLDEW>
front panel • 63
network requirements • 61
package contents • 60
rear panel • 61
Safe@Office <OLD500WADSL><OLDEWADSL>
front panel • 68
network requirements • 65
package contents • 65
rear panel • 66
Safe@Office 500 series
about • 1
features • 3
product family • 2
Safe@Office appliance
backing up • 749
cascading • 102
changing internal IP address of • 196
configuring Internet connection • 123
connecting to network printers • 103
controlling via the command line • 707
features • 3
firewall • 76
installing • 85
internal DNS server • 222
maintenance • 716
models • 2
mounting • 103
preparing for a wireless connection • 102
rapid deployment • 756
rebooting • 763
resetting to factory defaults • 759
restoring • 749
securing against theft • 105
security • 71

setting the time • 732
setting up • 107
status • 343
technical specifications • 795
Safe@Office appliance configuration
backing up to a USB flash drive • 751
exporting • 750
importing • 753
restoring from a USB flash drive • 755
Safe@Office Portal
elements • 118
initial • 111
logging in • 114
logging out • 653
remotely accessing • 116
using • 118
Secure HotSpot
customizing • 421
enabling/disabling • 420
quick guest users • 681
setting up • 419
using • 417
SecuRemote
explained • 602
installing • 609
SecuRemote Remote Access VPN Server
configuring • 605
explained • 597
security
about • 71
configuring port-based security • 411
configuring servers • 395
creating firewall rules • 398
defining a computer as an exposed host • 395
firewall • 392
Secure HotSpot • 417
SmartDefense • 447
Security Log
resetting • 381
viewing • 381
security policy
about • 389
default • 391
enforcement • 390
implementation • 390
planning • 390
setting up • 389
Sequence Verifier • 479
serial console
controlling appliance via • 710
using • 710
servers
configuring • 395
explained • 821

Service Center
connecting to • 587
disconnecting from • 595
refreshing a connection to • 594
service routing
explained • 239
services
Email Filtering • 556
software updates • 582
Web Filtering • 571
Setup Wizard • 111, 124
SIP • 494
Site-to-Site VPN gateways
explained • 597
PPPoE tunnels • 617
Small PMTU • 475
SmartDefense
categories • 456
configuring • 448
using • 447
SNMP
configuring • 727
explained • 727
software updates
checking for manually • 582
explained • 582
source routing
explained • 239
Spanning Tree Protocol
explained • 262
with WDS • 305
SSH
configuring • 713
explained • 713
Stateful Inspection
explained • 821
technology • 79
Static IP
configuring a connection • 131
Static NAT
explained • 225
using • 227
static routes
adding and editing • 240
explained • 239
using • 239
viewing and deleting • 243
viewing the routing table • 372
Status Monitor
viewing • 343
Strict TCP • 474
subnet masks
explained • 821
subscription services

explained • 587
starting • 587
viewing information • 593
Sweep Scan • 481
SynDefender • 477
Syslog logging
configuring • 722
explained • 722

T

Tag-based VLAN
about • 214
adding and editing • 220
deleting • 221
TCP
TCP, explained • 821
TCP/IP
setting up for MAC OS • 95
setting up for Windows XP/2000 • 90
Teardrop • 457
technical support
contacting • 70
Telstra
Telstra • 162
Traffic Monitor
configuring • 352
exporting reports • 354
using • 350
viewing reports • 351
traffic reports
exporting • 354
viewing • 351
Traffic Shaper
advanced • 291
enabling • 291
explained • 291
restoring defaults • 301
setting up • 293
simplified • 291
using • 291
troubleshooting • 789

U

UDP
explained • 822
URL
explained • 822
users
adding and editing • 676
adding quick guest HotSpot • 681
managing • 673
setting up remote VPN access for • 683
viewing and deleting • 682

V

Vendor-Specific Attribute
about • 684

configuring • 509
virtual access points (VAPs)
about • 214
adding and editing • 331
deleting • 221
VLAN
adding and editing • 217
configuring • 53
configuring port-based • 218
configuring tag-based • 220
configuring virtual access points • 331
deleting • 221
types • 214
VPN
explained • 597
Remote Access • 601
sites • 597
Site-to-Site • 599
tunnnels • 597
viewing IKE traces • 668
VPN Server
configuring • 603
SecuRemote internal • 602
types • 603
VPN sites
adding and editing • 617
deleting • 649
enabling/disabling • 649
logging in • 650
logging out • 653
types • 597
VPN tunnels
creation and closing of • 665
establishing • 650
explained • 822
viewing • 665
VStream Antispam
about • 523
configuring advanced settings • 555
configuring the Block List engine • 537
configuring the Content Based Antispam engine • 533
configuring the IP Reputation engine • 542
configuring the Safe Sender list • 552
default policy • 528
enabling/disabling • 529
header marking • 528
how it works • 526
rules • 545
viewing statistics • 531
VStream Antispam rules
adding and editing • 546
deleting • 552
enabling/disabling • 551

reordering • 551

types • 546

VStream Antivirus

about • 505

configuring • 505

configuring advanced settings • 518

configuring policy • 509

default policy • 506

enabling/disabling • 507

rules • 510

updating • 523

viewing database information • 508

VStream Antivirus rules

adding and editing • 510

deleting • 518

enabling/disabling • 517

reordering • 517

types • 510

W

WAN

cable • 99

load balancing • 190

WDS

explained • 305

links • 305

WDS links

configuring • 336

explained • 305

Web content filtering solutions

about • 561

comparison of • 561

Web Filtering • 571

Web rules • 563

Web Filtering

customizing the Access Denied page • 578

enabling/disabling • 571

excluding network objects from • 225

resetting to defaults • 577

selecting categories for • 573

snoozing • 574

temporarily disabling • 574

Web rules

adding and editing • 564

customizing the Access Denied page • 578

enabling/disabling logging • 570

reordering • 569

using • 563

viewing and deleting • 570

Welchia • 469

WEP • 303, 309

wireless networks

troubleshooting connectivity • 340

viewing statistics for • 368

wireless protocols
supported • 309
wireless stations
viewing • 368
Worm Catcher • 489

X

XBox LIVE • 500